

These Software as a Service Terms as entered into by and between Fluxx Labs, Inc. ("**Fluxx**") and the Customer (together with all Addenda attached hereto or referenced herein, the "**Terms**"), the Order to which these Terms are linked, any Statement(s) of Work and any other exhibits or attachments govern Customer's access to and use of the Fluxx System. Any initially capitalized terms used but not otherwise defined in these Terms shall have the meaning ascribed to such terms in the Order or in an attached or referenced addendum, as applicable. This Agreement is effective as of the Effective Date of the Order executed by both Fluxx and Customer.

## **1. Certain Definitions; Interpretation; Construction.**

Each following initially capitalized term has the meaning ascribed to such term herein. Whenever the words "include," "includes" or "including" are used in this Agreement, they shall be deemed to be followed by the words "without limitation." The terms "cash," "dollars" and "\$" mean United States dollars. All Addenda and Exhibits attached hereto shall be deemed part of this Agreement and included in any reference to this Agreement. Any singular term in this Agreement shall be deemed to include the plural, and any plural term the singular.

"**Addendum**" means each addendum attached hereto by the parties, including without limitation Addendum 1 (Support), Addendum 2 (Insurance) and Addendum 3 (Data Processing Agreement).

"**Agreement**" means the Order, these Terms, all Addenda and Exhibits attached hereto or referenced herein (which includes without limitation the Fluxx Privacy Notice) and each Statement of Work.

"**Authorized Territory**" means those countries and other geographic territorial regions identified in the Order from which Customer is authorized to access and use the Fluxx System on behalf of residents of such identified countries and other geographic territorial regions in accordance with the terms of this Agreement.

"**Customer Data**" means any information, documents or electronic files that Customer uploads to, or collects from its Users in, the Fluxx System, some of which may include Personal Data.

"**Data Processing Agreement**" or "**DPA**" means the Data Processing Agreement attached hereto as Addendum 3.

"**Documentation**" means the standard, online documentation for the Fluxx System that Fluxx makes available in the [knowledge base], the Fluxx System (Grantmaker) and through the community portal (community.fluxx.io), as each of the same may be revised and updated by Fluxx from time to time.

"**Effective Date**" means the Effective Date set forth on the Order.

"**Fees**" means, collectively, the Subscription Fee together with all SOW Fees.

"**Fluxx Privacy Notice**" means Fluxx's privacy policy and other attachments thereto or references therein attached hereto, each as non-materially updated by Fluxx from time to time, a current copy of which can be found at <https://www.fluxx.io/privacy-policy>.

"**Fluxx System**" means Fluxx's proprietary hosted grants management system that integrates customer relationship management and business process workflows (including any updates, revisions, enhancements, modifications, and derivative works thereof that may be provided hereunder), including the related services specified in the Order, the Addenda attached hereto and each Statement of Work.

**"Go-Live"** and **"Go-Live Date"** means the fully-configured and customized Fluxx System is made fully available to Customer's users in a production environment with all migrated data available in the Fluxx System, and the date on which the same occurs, respectively.

**"Law"** means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, decree, other requirement or rule of law of any federal, state, local, or foreign government or political subdivision thereof, or court, or tribunal of competent jurisdiction.

**"Order"** means the Software as a Service Order to which these Terms are attached.

**"Personal Data"** means information that, when used alone or with other relevant data, can identify an individual User (which by way of illustration but not limitation, might include name, address, email address, phone number, credit card number or passport number). Without limiting the generality of the foregoing, Personal Data includes any data relating to a User that constitutes "personal information," "personal data," or any term of similar import, under any applicable Data Protection Laws.

**"Process"** (and with correlative meanings, the terms **"Processed"** and **"Processing"**) means, with respect to Personal Data, the collection, use, disclosure, retention, storage, transfer or other processing thereof.

**"Services"** has that meaning set forth in the applicable Statement of Work.

**"SOW Fee"** means the fee that Customer must pay for services, as specified in each Statement of Work.

**"Statement of Work"** means each statement of work mutually executed by the parties setting forth the onboarding and/or configuration services relating to the Fluxx System to be provided by Fluxx, or any additional professional services to be provided by Fluxx, such as advanced configuration (configuration that requires integration, analysis, build and testing) and individual training. Each Statement of Work shall be attached hereto as an exhibit.

**"Subscription Fee"** means the annual fee, as set forth in the Order, that Customer pays in advance for the right to access and use the Fluxx System during the Subscription Term.

**"Subscription Term"** means the period set forth in the Order, so long as Customer remains current in payment of all Subscription Fees.

**"User"** means a named individual to whom Customer has granted access to use the Fluxx System on Customer's behalf or in connection with Customer's business, regardless of whether or not the User actually accesses the Fluxx System, subject to the terms of this Agreement.

## **2. Access to and Use of Fluxx System; Ownership of Fluxx System**

a. Subject to the terms of this Agreement, Fluxx hereby grants to Customer a non-exclusive, non-transferable, non-sublicensable, limited right during the Subscription Term to permit Customer's Users to access remotely via the Internet and use the Fluxx System, solely within the Authorized Territory and on behalf of persons within the Authorized Territory, only for Customer's internal purposes and solely in accordance with the Documentation.

b. As between Fluxx and Customer, Fluxx is and shall remain the owner of the Fluxx System and all portions thereof and Customer acknowledges and agrees that Fluxx is and shall remain owner of all right, title and interest in and to all intellectual property rights (including all derivatives or improvements thereof) in the Fluxx System, including without limitation any invention or discovery related to the Fluxx System that may be made as a consequence of Customer's accessing or using the Fluxx System. Customer further acknowledges and agrees that (i) Fluxx and the Fluxx System may use machine learning ("**ML**"), directly and/or indirectly, to process Customer Data in efforts to improve the Services and/or provide better data security and malware detection, (ii) all algorithms, software applications, models, statistical techniques, pattern recognition and data resulting from such ML shall be completely anonymized such that neither the

identity of Customer nor its Users can be ascertained therefrom ("**ML Results**") and (iii) all rights, title and interest in and to all ML Results shall be owned solely by Fluxx. If Customer or any of Customer's Users provide to Fluxx any suggestions, enhancement requests, feedback, recommendations, or other information relating to the Fluxx System ("**Feedback**"), then Fluxx may freely use and exploit such Feedback in any manner and for any purpose whatsoever without any consideration to Customer or its Users or any other obligations or restrictions. Fluxx is providing a limited term subscription to access and use the Fluxx System during the Subscription Term. Customer acknowledges that access to, and use of, the Fluxx System is limited to the scope of the express provisions set forth in this Section 2.b. and that there are no implied licenses; all rights not expressly granted under this Agreement are reserved by Fluxx.

c. Except as expressly permitted hereunder, Customer shall not and shall not permit any person (including, without limitation, Users), directly, indirectly, alone, or with another party do or attempt to do any of the following: (i) copy, disassemble, reverse engineer, decompile, or attempt to derive the source code of the underlying software or technology providing the Fluxx System; (ii) modify, create derivative works based upon, or translate the Fluxx System; (iii) license, sell, rent, lease, transfer, grant any rights in or otherwise commercially exploit the Fluxx System in any form with any other party; (iv) upload Customer Data or other content that misappropriates or violates any third party proprietary rights or privacy rights; (v) remove, modify or otherwise tamper with notices or legends on the Fluxx System or Documentation; (vi) interfere with the operation or functionality of the Fluxx System; (vii) attempt to probe, scan, penetrate, breach or test the vulnerability of the Fluxx System or disable or circumvent the Fluxx System's security or authentication measures without Fluxx's prior, written authorization; or (viii) use or access the Fluxx System for the purpose of building a competitive product or service.

d. Customer is and shall remain owner of all right, title and interest in the Customer Data. Customer hereby grants to Fluxx, a nonexclusive, non-transferable (except if authorized under Section 13(c) below), right and license to use, host, copy, transmit, modify and display the Customer Data for purposes of (i) enabling and improving Customer's use of the Fluxx System; (ii) compiling and analyzing data concerning usage of the Fluxx System that has been aggregated with similar data relating other Fluxx customers and anonymized so that it does not specifically identify Customer or its Users; and (iii) generating ML Results. To the extent legally permissible, Customer will be responsible for any costs arising in connection with Fluxx's or its vendor's or licensor's provision of assistance in correcting, blocking or deleting Customer Data.

e. Customer is responsible for ensuring that Customer and Customer's Users' use of the Fluxx System is in compliance with all applicable Laws and Customer acknowledges that Customer assumes all risk arising from any such use that is not compliant with applicable Laws. Without limiting the generality of the foregoing, Customer is solely responsible for making necessary disclosures and providing notice to, and obtaining necessary consents from, Customer's administrative Users and non-administrative Users alike.

f. Customer is solely responsible for maintaining the security of all credentials, including but not limited to usernames and passwords granted to it, for the security of its information systems used to access the Fluxx System, and for its Users' compliance with the terms of this Agreement. Fluxx will act as though any electronic communications it receives from a Customer e-mail address or using a User's credentials have been sent by Customer. Customer will immediately notify Fluxx if it becomes aware of any loss or theft or unauthorized use of any of Customer's credentials.

g. Customer will promptly notify Fluxx in writing of any unauthorized use that comes to Customer's attention. If there is unauthorized use by anyone who obtained access to the Services or Fluxx System directly or indirectly through Customer, then Customer will take all steps reasonably necessary to terminate such unauthorized use. Customer will cooperate and assist with any actions taken by Fluxx to prevent or terminate unauthorized use of the Services or Fluxx System

h. Fluxx has the right at any time to temporarily suspend access for any User or Customer, without prior notice, if Fluxx reasonably believes suspension is necessary to preserve the security, integrity or accessibility of the Fluxx System.

### 3. Statements of Work

Fluxx will use commercially reasonable efforts to provide to Customer the onboarding and/or configuration services, or additional professional services, such as advanced configuration (configuration that requires integration, analysis, build and testing) and individual training relating to the Fluxx System, as described in the applicable Statement of Work, and Customer will pay Fluxx the SOW Fee as set forth in the applicable Statement of Work.

### 4. Subscription Fees and SOW Fees; Payment

Customer shall pay to Fluxx the Subscription Fees specified in the Order, in accordance with the payment terms set forth in such Order.

Customer shall pay to Fluxx the SOW Fees specified in each Statement of Work, in accordance with the payment terms set forth in such Statement of Work.

Any failure to pay Fees within 30 days of the applicable due date may constitute a material breach by Customer under this Agreement, and any such unpaid Fees will accrue a late payment fee equal to the interest rate established by the Secretary of the Treasury as provided in [41 U.S.C. 7109](#), which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

Customer shall reimburse Fluxx for all travel and other expenses set forth in the Statement of Work and pre-approved by Customer in writing in accordance with FAR 31.205-46 and the Federal Travel Regulation (FTR), and Fluxx will provide documentation supporting any such expense reimbursement upon written request.

### 5. Confidentiality

**"Confidential Information"** means any proprietary information, technical data, trade secrets or know-how, including but not limited to research, product plans, products, services, suppliers, supplier lists, customers, customer lists, markets, software, developments, inventions, processes, formulas, technology, designs, drawings, engineering, hardware configuration information, marketing, finances, or other business information disclosed by one party ("**Disclosing Party**") to the other party ("**Receiving Party**"), either directly or indirectly, in writing or orally that (i) is marked or designated as confidential or (ii) in light of the nature of the information itself or the circumstances of its disclosure, a reasonable person should consider to be confidential. For purposes of this Agreement, Customer Confidential Information shall include all Customer Data, and Fluxx Confidential Information shall include the Fluxx System, underlying software technology providing the Fluxx System, Documentation and the terms of this Agreement and the related Orders. Each Receiving Party agrees that it will (1) hold in strict confidence the Confidential Information of the Disclosing Party, (2) not disclose the Confidential Information of the Disclosing Party to any third party without the Disclosing Party's written authorization (except to the extent expressly permitted hereunder) and (3) use the Confidential Information of the Disclosing Party only for the purposes expressly permitted by this Agreement, and no other purpose. The Receiving Party will only permit access to the Disclosing Party's Confidential Information to the Receiving Party's employees, contractors, advisors and third-party vendors (which includes, where Fluxx is the Receiving Party, those that assist Fluxx with the design, provision, maintenance or support of the Fluxx System or related services) who have a need to know and who have signed or are bound by confidentiality obligations or agreements containing terms at least as restrictive as those contained in this Agreement. Each party will maintain confidentiality and prevent accidental or other loss or disclosure of any Confidential Information of the other party with at least the same degree of care as it uses to protect its own Confidential Information, but in no event with less than reasonable care. A Receiving Party's obligations of confidentiality under this Agreement will not apply to information that such party can establish (i) is generally known within the industry without the breach of any agreement or fiduciary duty or the violation of any Law, (ii) was known to the Receiving Party prior to the time of disclosure by the Disclosing Party without the breach of any agreement or fiduciary duty or the violation of any Law by the Receiving Party, (iii) has been rightfully received by the Receiving Party from a third party who is authorized

to make such disclosure; or (iv) was independently developed by the Receiving Party without use or reference to the Disclosing Party's Confidential Information. Each party recognizes and acknowledges that any use or disclosure of the Confidential Information by the Receiving Party in a manner inconsistent with the provisions of this Agreement might cause the Disclosing Party irreparable damage for which remedies at Law may be inadequate.

## 6. Privacy, Security and Data Protection

a. Fluxx will maintain administrative, physical and technical safeguards reasonably designed for the protection of the security, confidentiality and integrity of Customer Data as attested to and verified in Fluxx's recurring SOC 2 Type 2 report. Customer acknowledges and agrees that Fluxx may share Customer Data with third-party vendors that assist Fluxx with the performance of this Agreement, in which case Fluxx shall take reasonable precautions to ensure that said Customer Data is treated by any authorized third-party vendor with at least the same degree of care as it uses to protect its own Confidential Information.

b. Customer further acknowledges that the Fluxx System is not designed (or intended) to process or manage any (i) protected health information under HIPAA, or other similarly sensitive personal information, and/or (ii) special categories of personal data as set forth in Article 9 of the GDPR (defined in the Fluxx Privacy Notice) with respect to any natural person (collectively "**Sensitive Data**"). Customer shall not permit or cause its Users to disclose any Sensitive Data to the Fluxx System. Customer assumes all risk arising from the disclosure or use of any Sensitive Data on or with the Fluxx System, including the risk of any inadvertent disclosure or unauthorized access thereto.

c. Each party shall comply at all times with applicable Data Protection Laws, as that term is defined in the DPA attached hereto. In the event that any applicable Data Protection Laws require the parties to cooperate in order to address the rights of any individuals, the parties shall take all reasonable steps to cooperate and comply with such obligations.

d. To the extent required by Data Protection Laws, each party shall maintain and make available a privacy policy that complies with such Laws. Fluxx's privacy policy is attached here to and currently located at: [Fluxx's Privacy Policy \(https://www.fluxx.io/privacy-policy\)](https://www.fluxx.io/privacy-policy).

e. Where Fluxx provides Customer with direct access to a virtual machine or database server with sufficient permissions to allow the creation or modification of applications or databases on that machine, the Customer is responsible for the security of that machine and the content on that machine. This includes user provisioning, logical access to, and the confidentiality, integrity, and availability of the data or service that relies upon that machine.

f. Where Fluxx provides custom systems to the Customer, the Customer is responsible for ensuring that access configurations align with Customer's expectations.

g. Customer is and shall be responsible for the user provisioning, logical access to and security of the Customers' users use of the Fluxx System, and Customer will report to Fluxx any issues or security concerns that might affect the Customer's use of the Fluxx System in a timely manner, and in all events within 72 hours of becoming aware of such a concern.

h. To the extent Customer, in its use of the Services, does not have the ability to correct, amend, block, transfer, or delete Customer Data as required by Data Protection Laws, Fluxx will comply with any commercially reasonable request by Customer to facilitate such actions. To the extent legally permissible, Customer will be responsible for any costs arising in connection with such correction, amending, blocking, transferral or deletion activities of Fluxx or its vendors or licensors.

i. Customer may request in writing the disposal of Customer Data upon expiration or the earlier termination of the Agreement. Termination notice will be sent via email to the assigned Customer Success Manager (CSM) or, if no CSM has been assigned, to the Customer success team.

## **7. Support Services**

Fluxx will use commercially reasonable efforts to provide support services (the "**Support Services**"), as further described in Addendum 1 (Support) attached hereto.

## **8. Limited Warranty; Disclaimer of Other Warranties**

a. Fluxx warrants to Customer that during the Subscription Term: (i) the Fluxx System will operate substantially in accordance with the Documentation when used as directed; and (ii) such functionality will not be materially decreased. Fluxx shall remedy any failure to conform to such warranty by providing the Support Services to modify the Fluxx System to achieve the warranted functionality, provided that any such nonconformance: (1) is sufficiently described in writing and reproducible by Fluxx; and (2) is not the result of use by Customer or Users of the Fluxx System in a manner inconsistent with this Agreement and/or Documentation. If Fluxx is unable to meet the foregoing warranty obligations, then Customer's sole and exclusive remedy shall be to terminate the Agreement for breach in accordance with Section 12(b) below and Fluxx will refund to Customer on a pro-rata basis all pre-paid Fees attributable to unused portion of the Subscription Term for the applicable Order.

b. EXCEPT FOR THE WARRANTIES EXPRESSLY SET FORTH IN SECTION 8.a. ABOVE, THE SERVICES ARE PROVIDED SOLELY ON AN "AS IS" AND "AS AVAILABLE" BASIS, WITHOUT REPRESENTATIONS OR WARRANTIES OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, FLUXX EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO: IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND TITLE AND NON-INFRINGEMENT; AND THAT THE OPERATION OR USE OF THE SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE.

## **9. Limitation of Liability**

a. In no event shall either party be liable to the other party for any incidental, indirect, exemplary, special, punitive or consequential damages, however caused and under any circumstances, or for any lost profits, revenue or savings, or the loss of use of any data, even if a party has been advised of, knew or should have known of, the possibility thereof.

b. To the maximum extent permitted by applicable Law, Fluxx's and its licensor's or supplier's total aggregate liability for any and all claims, losses or expenses (including attorneys' fees) arising out of or in connection with this Agreement, whether based in contract, negligence, strict liability, warranty, misrepresentations, other torts or any other theory of liability, will be limited to the Fees actually paid by Customer to Fluxx during the twelve (12) month period immediately preceding the act or omission first giving rise to the liability.

c. NOTWITHSTANDING THE FOREGOING LIMITATIONS IN SECTIONS 9(a) AND 9(b) ABOVE, NO LIMITATION OF LIABILITY SHALL APPLY TO THE EXTENT THE CLAIM RESULTS FROM (I) INFRINGEMENT OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, (II) GROSS NEGLIGENCE, FRAUD OR WILLFUL MISCONDUCT BY THE OTHER PARTY, (III) CUSTOMER'S OR ITS USERS' USE OF THE FLUXX SYSTEM FOR ANY UNLAWFUL PURPOSE OR IN BREACH OF CUSTOMER'S LICENSE RIGHTS UNDER THIS AGREEMENT, (IV) CUSTOMER'S OR ITS USERS' PROVISION OF, AND AUTHORIZATION GRANTED TO FLUXX TO ACCESS, STORE OR USE PURSUANT TO THIS AGREEMENT, CUSTOMER DATA IN VIOLATION OF APPLICABLE LAWS OR REGULATIONS, OR (V) BREACH OF CUSTOMER'S PAYMENT OBLIGATIONS. These exclusions are meant to apply to the fullest extent permitted by applicable Law and regardless of the failure of any specific remedy.

## 10. Indemnification

a. Fluxx Indemnification. Fluxx agrees to have the right to intervene to defend, indemnify and hold harmless Customer, its trustees, beneficiaries, employees and agents (collectively, "**Indemnified Party**"), from and against all claims, demands, damages, liabilities, losses and expenses, including reasonable attorneys' fees and expenses, to the extent resulting from any third party claim or suit against Customer based on a claim that the technology used to provide the Fluxx System infringes any United States patent, copyright, trademark or trade secret and Fluxx shall pay any final judgment entered against the indemnified party in any such proceeding or agreed to in settlement. If Customer's use of the Fluxx System is, or is likely, in Fluxx's reasonable determination, to be infringing, then Fluxx may, without limiting its indemnity obligations hereunder, procure the right for Customer to continue to use the Fluxx System or modify the Fluxx System in a manner that has materially equivalent functionality so as to avoid such infringement. If the foregoing options are not available on commercially reasonable terms and conditions, Fluxx may terminate the Agreement upon written notice and refund to Customer on a pro-rata basis all pre-paid Fees attributable to the unused portion of the Subscription Term for the applicable Order. Fluxx will not be responsible for any infringement claims based upon (i) the use of Customer Data, or other material or software not furnished by Fluxx; (ii) use by Customer or Users of the Fluxx System in a manner inconsistent with this Agreement and/or Documentation. THIS SECTION 10(A) STATES FLUXX'S ENTIRE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR INTELLECTUAL PROPERTY INFRINGEMENT AND MISAPPROPRIATION CLAIMS RELATED TO THE FLUXX SYSTEM. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

b. Indemnification Procedures. The following procedural requirements will apply to the Indemnified Party seeking indemnification from Fluxx. To avail itself of the foregoing indemnification, the Indemnified Party will: (i) promptly notify Fluxx in writing of the claim for which indemnification is sought ("**Claim**") (provided that any delay in such notice that does not materially prejudice Fluxx in its defense of such Claim will not relieve Fluxx of its obligations hereunder); (ii) provide Fluxx, at Fluxx's expense, with all reasonable information and assistance to defend or settle the Claim; and (iii) grant Fluxx with the necessary authority and control of the defense or settlement of the Claim.

## 11. Insurance

Fluxx shall obtain and maintain during the term of this Agreement, at its own expense, the insurance policies and coverage as set forth in Addendum 2 attached hereto.

## 12. Term and Termination

a. The term of this Agreement commences on the Effective Date of the Order and, unless earlier terminated pursuant to this Agreement, continues until the Subscription Term specified in such Order expires. The term of this Agreement may be renewed for successive one-year Subscription Terms in the event that (i) Customer provides notice of intent to renew at least thirty (30) days in advance of the end of the then-current Subscription Term and (ii) the parties mutually agree in writing to a new Subscription Term.

b. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Fluxx shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

c. Upon termination or expiration of this Agreement: (i) the usage rights granted under Section 2(a) immediately terminate; (ii) each party will, upon written request, promptly return to the other party any Confidential Information of the other party in its possession, custody or control; and (iii) Fluxx will extract Customer Data from the Fluxx System and make a copy available to Customer for thirty (30) days after the date of termination. Sections 2(b) through 2(e) inclusive, 4, 5, 6, 8(b), 9, 10, 12(c) and 13 and the applicable definitions in Section 1 shall survive termination of this Agreement.

## 13. Miscellaneous

a. Notices regarding this Agreement to Fluxx shall be in writing and sent by electronic mail, first class mail, or overnight courier at the address provided at that time on Fluxx's website. Fluxx may give notice by means of posting notice on the Fluxx System, by electronic mail to Customer's e-mail address on record with Fluxx, or by written communication sent by first class mail or overnight courier to Customer's address on record in Fluxx's account information. All notices shall be deemed to have been given three days after mailing or posting (if sent by first class mail), upon delivery in the case of courier, or 12 hours after either sending by e-mail or posting on the Fluxx System.

b. Customer grants Fluxx the right to use its name and logo in customer lists on its website, commercial advertisements and promotional materials for the sole purpose of indicating that Customer is a user of the Fluxx System, provided that Fluxx complies with Customer's written trademark usage policy provided to Fluxx and to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

c. Neither party may assign any of its rights hereunder or this Agreement, whether by operation of Law or otherwise, without the other party's prior written consent, such consent not to be unreasonably delayed, conditioned or withheld. Subject to the foregoing, the Assignment will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

d. In accordance with GSAR Clause 552.212-4(f), Fluxx will not be liable or responsible for any failure to perform, or delay in performance of, any of Fluxx's obligations under this Agreement that is caused by a Force Majeure Event, where "**Force Majeure Event**" means an act or event beyond Fluxx's reasonable control, including without limitation acts of God, war (whether or not actually declared), armed conflict or the serious threat of the same, hostility, blockade, military embargo, sabotage, insurrection, rebellion, act of a public enemy, riot or other act of civil disobedience, governmental act, judicial action, explosion, act of terrorism or threat thereof (including cyberterrorism), natural disaster (including without limitation asteroid strikes or volcanic activity), violent storm (including without limitation hurricanes, tornadoes or blizzards), atmospheric disturbance (including without limitation geomagnetic storm, solar flare or sun outage with respect to electricity grids, transformers and satellite transmissions), destruction by lightning, fire, earthquake, tsunami, flood, plague, epidemic, pan- epidemic, quarantine, civil commotion, strike or lockout or labor dispute (excluding for the avoidance of doubt strikes of Fluxx's staff), satellite malfunction, prolonged internet outage, communications line failure or power failure or impossibility of the use of public or private transport, communication systems, the internet or third party hosting providers (e.g. AWS).

e. Any determination of invalidity or unenforceability of any one provision shall have no effect on the continuing force and effect of the remaining provisions. The failure of either party to enforce any right or provision of this Agreement shall not constitute a waiver of such right or provision.

f. This Agreement shall be governed by the Federal Laws of the United States.

g. This Agreement constitutes the entire agreement of the parties regarding the subject matter hereof and supersedes any prior written agreements or understandings between the parties with respect to the Fluxx System. The preprinted terms of any purchase order or similar document provided by Customer shall be void and of no force or effect. This Agreement may not be amended except by a writing signed by each party.

## Addendum 1 - Support

### 1) Support

- a) **Support Commencement Date.** The Support Services will commence on the Subscription Start Date and continue until termination of the Agreement.
- b) **Customer Contacts.** All Support Services inquiries will be directed to Fluxx from employees or consultants identified in writing to Fluxx by Customer. All Support Services inquiries should be directed to the electronic mail interface and/or telephone number established for Customer. Customer will use commercially reasonable efforts to minimize repetitive Support Services inquiries for the same error. All support requests will be submitted in the format provided by Fluxx to Customer described herein.
- c) **Support Services Hours.** Fluxx will deliver ongoing Support Services from 1:00 a.m. to 5:00 p.m. Pacific Time (excluding applicable public and company holidays) (the "**Business Hours**"). Support requests for service during normal business hours should be submitted by Customer to the person identified by Fluxx, which identification shall be done promptly upon SOW execution.
- d) **Technical Support.** Without limiting any other obligations hereunder, Fluxx will provide consultation, instruction, and basic technical support services (consisting of minor configuration changes, Fluxx System upgrades, and troubleshooting) to Customer regarding the Fluxx System ("**Technical Support**"). In response to requests from Customer, Technical Support may be delivered by electronic mail, telephone, remote support, and/or Internet-delivered answers during the Subscription Term.
- e) **Advanced Services.** These optional services, which include audit, advanced configuration (configuration that requires analysis, build and testing), office hours and training certification packaged can be requested, scoped and managed under a separate Statement of Work.

## **Addendum 2 - Insurance**

- a. Fluxx shall obtain and maintain during the term of this Agreement, at its own expense:
  - i. A comprehensive general liability insurance policy with limits of liability of at least \$1,000,000, combined for bodily injury and property damage, \$1,000,000 for automobile liability and \$2,000,000 excess umbrella liability coverage.
  - ii. A cyber liability insurance policy, including first party and third-party coverage, with limits no less than \$1,000,000 per occurrence and \$3,000,000 in the aggregate for all claims each policy year.
  - iii. An errors and omissions/professional liability insurance policy with limits no less than \$1,000,000 per occurrence and \$3,000,000 in the aggregate for all claims each policy year.
- b. Upon written request of Customer, Fluxx will deliver a Certificate of Insurance that will confirm Fluxx has the policies and coverage in place as required above. Fluxx shall provide proof of Workers Compensation coverage in the amounts as required by Law.

## Addendum 3 - Fluxx Labs Inc. Data Processing Agreement

This Data Processing Agreement ("**DPA**"), effective as of the Effective Date set forth on the Order, sets forth the terms and conditions relating to the privacy, confidentiality, security and protection of Personal Data (as defined below) associated with Services rendered by Fluxx to Customer pursuant to that certain Software as a Service Order, the Software as a Service Terms (and addenda thereto), and the Statement(s) of Work entered into by and between the Customer and Fluxx (collectively, the "**Agreement**"). Customer and Fluxx may collectively be referred to as the "**Parties**" and each, individually, as a "**Party**." Initially capitalized terms used but not otherwise defined in this DPA shall have the meaning ascribed to such terms in the Software as a Service Order, the Software as a Service Terms or any Statement of Work.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

### 1. Definitions

**1.1 "Affiliate"** means any entity that now or in the future directly or indirectly controls, is controlled by, or is under common control or ownership for as long as such control exists, where "control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct, influence or cause the direction of the management policies of an entity, whether through the ownership of voting securities, by contract, or otherwise.

**1.2 "Data Controller"** means the entity that determines the purposes and means of Processing.

**1.3 "Data Processor"** means the entity that Processes Personal Data on behalf of the Data Controller.

**1.4 "Data Protection Laws"** means all Laws currently in effect and as they become effective within the Authorized Territory relating to the privacy, confidentiality, security or protection of Personal Data that apply to the parties in connection with providing or receiving the Services, as applicable, within the Authorized Territory.

**1.5 "Data Subject"** means an identified or identifiable natural person to which the Personal Data pertains.

**1.6 "Personal Data"** means any data, information or record that is Processed in connection with the Agreement (i) relating to an identified or identifiable natural person, or (ii) that identifies, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, regardless of the media in which it is maintained.

**1.7 "Personal Data Breach"** means the breach of security leading or reasonably expected to lead to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data Processed under the Agreement.

**1.8 "Process," "Processing" or "Processed"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated 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.

**1.9** "Sell" or "Selling" shall have the meaning ascribed to it in the applicable Data Protection Law.

**1.10 "Standard Contractual Clauses" or "SCCs"** means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, and implemented by the European Commission decision 2021/914, dated 4 June 2021.

**1.11 "Subprocessor"** means other processors used by Fluxx to process Personal Data.

**1.12 "Supervisory Authority"** means (i) an independent public authority that is established by an EU member state pursuant to Article 51 of the EU GDPR; or (ii) a government regulator or enforcement authority that has regulatory or enforcement authority with respect to the privacy, confidentiality, security or protection of Personal Data.

## **2. Nature of Data Processing**

**2.1 Processing Limitations.** Fluxx will only Process Personal Data in accordance with (i) Customer's written instructions as set forth in, or pursuant to, the Agreement and (ii) Annex I to the SCCs, if applicable. Fluxx will not use or otherwise Process Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes including Selling, or (c) any other purpose. If applicable Law requires Fluxx (or, for avoidance of doubt, any Subprocessor) to conduct Processing that is or could be construed as inconsistent with Customer's instructions, Fluxx will promptly notify Customer of such inconsistency prior to commencing (or continuing) the Processing, unless notification is prohibited by Law.

**2.2 Role of the Parties.** Customer and Fluxx agree that Customer is the Controller of Personal Data and Fluxx is the Processor. Fluxx agrees that the Agreement (including any applicable updates), is Customer's complete documented instructions to Fluxx for the Processing of Personal Data.

## **3. Compliance with Applicable Law**

Fluxx will comply with Data Protection Laws and, with respect to Laws other than those relating to the privacy, confidentiality, security or protection of Personal Data, such other applicable Laws and regulations applicable to its performance under the Agreement. This DPA is not meant to reduce the level of protections applicable to each Data Subject. In the event of any conflict or inconsistency between the DPA terms and any other terms in the Agreement, the DPA terms shall prevail. As required by clause 5 of the SCCs (if applicable), the SCCs prevail over any other term of this DPA and terms of the Agreement.

## **4. Subprocessors**

**4.1 Appointment of Subprocessors.** Fluxx may engage Subprocessors, including its Affiliates to provide services on its behalf. When engaging a Subprocessor, Fluxx will ensure via a written agreement that (i) the Subprocessor may access and use Personal Data only to deliver the services Fluxx has retained them to provide and is prohibited from using Personal Data for any other purpose and (ii) that Subprocessor provides for, in substance, substantially equivalent data protection obligations as those binding Fluxx under this DPA and (if applicable) the SCCs. As further described in Annex III to the DPA, Fluxx agrees to oversee Subprocessors to ensure these contractual obligations are met.

**4.2 New Subprocessors.** If Fluxx engages new Subprocessors, Fluxx will give Customer notice of any new Subprocessor (in accordance with clause 9(a) of the SCCs if applicable). If Customer raises a commercially reasonable objection to a new Subprocessor in writing within 10 business days after receipt of notice, and Fluxx is unable to resolve that objection in a reasonable amount of time, then Customer may terminate the affected services, which cannot be provided by Fluxx without the use of the new

Subprocessor, by providing, before the end of the relevant notice period, written notice of termination, and shall be entitled to pro rata refunds for fees paid for the applicable terminated services.

**4.3 Liability.** Subject to Section 10.2 below, Fluxx is responsible for its Subprocessors' compliance with Fluxx's obligations as outlined in the DPA and Fluxx shall remain liable for Subprocessors' acts or omissions that result in a breach of the DPA.

## **5. Security**

**5.1 Security Measures.** Fluxx will implement and maintain technical and organizational security measures including, as appropriate: (i) encryption and pseudonymisation; (ii) such measures designed to provide the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) such measures designed to provide the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of those measures. If applicable, Fluxx represents and warrants it has implemented the security measures described in the attached Annex II to the SCCs to protect Personal Data.

**5.2 Access to Personal Data and Confidentiality.** Fluxx will implement and maintain measures designed to ensure that Personal Data is only available to those who have a legitimate business need to access the Personal Data, who are bound by legally enforceable confidentiality obligations, and who will only Process Personal Data in accordance with Customer's instructions. Fluxx shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Personal Data in accordance with applicable Data Protection Laws and industry standards.

**5.3 Personal Data Breach Response and Notification.** If Fluxx becomes aware of a Personal Data Breach affecting Personal Data while Processed by Fluxx, Fluxx will promptly and within the period required by applicable Data Protection Laws (i) notify Customer of the Personal Data Breach ; (ii) investigate the Personal Data Breach and provide Customer with detailed information about the Personal Data Breach; and (iii) take reasonable steps to mitigate effects and to minimize any damage resulting from the Personal Data Breach. Notification(s) of Personal Data Breaches will be sent to Customer according to the notice provisions of the Agreement. If according to the Customer's assessment, a Personal Data Breach affecting Personal Data should be disclosed or reported to a third party, including Data Subjects, Supervisory Authorities or governmental authorities, Fluxx will fully cooperate with and assist Customer in such reporting or disclosure.

## **6. Audits/Inspections**

**6.1** Fluxx will conduct audits of its security controls applied to processing Personal Data (and, if applicable, of the Processing activities covered by the SCCs), as follows:

Each audit will be performed according to the rules of the accreditation body for each applicable control standard or framework.

Each audit will be performed by qualified, independent, third-party security auditors at Fluxx's selection and expense.

**6.2 Audit Summaries.** Each audit will result in the generation of an audit report ("**Fluxx Data Protection Audit Report**"), the summary of which Fluxx will make available to Company upon written

request. The summary of the Fluxx Data Protection Audit Report will be Fluxx's Confidential Information and the summary, as well as any content of the Fluxx Data Protection Audit Report, will be subject to non-disclosure and distribution limitations of Fluxx and the auditor.

## **7. Fluxx's Cooperation Obligation**

**7.1 Cooperation.** Fluxx will provide assistance to Customer to allow Customer to comply with its own obligations under Data Protection Laws with respect to Personal Data. Such assistance may include, without limitation, (i) responding to Data Subjects' requests to exercise their rights under Data Protection Laws; (ii) assistance with Customer's performance of a data protection impact assessment and, if necessary, prior consultation with the competent supervisory authority, with respect to the Processing of Personal Data under this DPA; and (iii) responding to requests or investigations of Customer by a Supervisory Authority, with respect to the Processing of Customer's Personal Data under the Agreement.

**7.2 Third-Party Access Requests and Complaints; Data Subject Requests.** Fluxx will not disclose or provide access to Personal Data except: (i) as Customer directs, (ii) as described in this DPA; or (iii) as required by Law, and in any event in accordance with the relevant clauses of the SCCs (where applicable). In connection with a product or service for which Customer is the Controller Fluxx will promptly notify Customer within five (5) days of any request or complaint from a Supervisory Authority, public authority, Data Subject or other third party relating to Personal Data or Customer's obligations under Data Protection Laws unless Fluxx reasonably determines that such notice is prohibited by Law. Fluxx will attempt to redirect the third party to request the Personal Data directly from Customer and will provide Customer with a copy of the request unless legally prohibited from doing so. If unable to redirect the request, Fluxx will reject it unless required by Law to comply, exercising any challenges as may be applicable to the request before responding (i.e. overbroad). If applicable, Fluxx will act in accordance with clauses 14 and 15 of the SCCs in handling requests.

**7.3 Requests.** Fluxx shall comply with requests by Customer to assist with Customer's response to such a Data Subject request.

## **8. Data Retention, Return and Deletion**

**8.1 Retention.** Fluxx will not retain Personal Data any longer than is reasonably necessary to accomplish the intended purposes for which the Personal Data was Processed pursuant to the Agreement.

**8.2 Return and Deletion.** When Personal Data is no longer necessary for the purposes set forth in the applicable Agreement or promptly upon the expiration or termination of the Agreement, whichever is earlier, or at an earlier time as Customer requests in writing, Fluxx will (i) provide a mechanism for Customer to obtain all Personal Data in a format mutually agreed upon by the Parties; and (ii) destroy all the Personal Data in Fluxx's possession or control. The foregoing obligations will also apply to Personal Data held by Subprocessors. Fluxx will provide a certification of destruction if requested. If applicable Law does not permit Fluxx to comply with the return or destruction of Personal Data, Fluxx agrees such retained Personal Data shall remain subject to the terms of this DPA and the SCCs and it shall return or destroy such Personal Data when permitted by applicable Law.

## **9. International Data Transfers**

**9.1 Transfer Mechanism.** If the services and/or products provided by Fluxx under the Agreement involve an international transfer of Personal Data from the EEA, Switzerland, or the United Kingdom to

countries which are deemed to provide inadequate levels of data protection ("Other Countries"), if required by Data Protection Laws, the Parties shall: (i) execute the model clauses adopted by the relevant data protection authorities of the European Commission or the UK Secretary of State as set forth in this section (if applicable); or (ii) comply with any of the other mechanisms provided for under Data Protection Laws for transferring Personal Data to such Other Countries.

**9.2 EU SCCs.** The Parties agree: to enter into the SCCs as set out in Attachment 1, for transfers of Personal Data from Customer or its Affiliates established in the EEA, as a data controller, to Fluxx established in a country outside the EEA, as a data processor as set out in Module II of the European Commission decision 2021/914, dated 4 June 2021 ("Controller to Processor SCCs" or "Module II"). The Controller to Processor SCCs will only apply to Personal Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for Personal Data. Personal Data that Fluxx processes on Customer's behalf may only be disclosed to a third party located outside the EEA in accordance with clause 8.8 of the Controller to Processor SCCs.

**9.3 UK Model Clauses.** The Parties agree that for transfers of Personal Data from the United Kingdom, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK ICO under S119A(1) Data Protection Act 2018 and in force March 21, 2022 (the "UK Addendum"), shall apply. The start date in Table 1 of the UK Addendum shall be the date that the Parties have executed Annex A. The selection of modules and optional clauses shall be as described with respect to the EU SCCs, subject to any revisions or amendments required by the UK Addendum. Where Customer is established in the United Kingdom or falls within the territorial scope of application of UK Data Protection Laws, the Information Commissioner's Office shall act as competent supervisory authority. All other information required by Tables 1-3 is set forth in the SCC Annexes in this DPA. For the purposes of Table 4, the parties agree that both the Importer and Exporter may end the UK Addendum.

**9.4 Swiss Data Transfers.** The Parties agree that for transfers of Personal Data from Switzerland, the terms of the EU SCCs shall be amended and supplemented as specified by the relevant guidance of the Swiss Federal Data Protection and Information Commissioner, and the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner.

## **10. Indemnification; Liability**

**10.1** Fluxx will defend, indemnify and hold Customer, its Affiliates and their respective officers, directors, employees, agents, customers and representatives (collectively, the "**Customer Indemnified Parties**") harmless from and against any liability, damages, costs, and expenses, including without limitation reasonable attorneys' fees, fines and penalties or investigative costs to the extent arising directly from a Personal Data Breach resulting directly from Fluxx's failure to comply with this DPA. Fluxx's obligations under this Section will be subject to the limitations on liabilities, damages, costs or expenses set forth in Section 10.2 below with respect to amounts payable to the Customer Indemnified Parties by Fluxx.

**10.2** Notwithstanding anything in this DPA (including without limitation any document incorporated in this DPA by reference) to the contrary, except for damages for bodily physical injury, death, damage to real or tangible personal property or for gross negligence, intentional misconduct or fraud: (i) in no event shall Fluxx be liable to Customer, its Affiliates and its and their respective officers, directors, employees,

agents, customers and representatives, on any theory of liability, whether in contract, strict liability or tort (including negligence or otherwise), for any loss or unavailability of or damage to data, lost revenue, lost profits, failure to realize expected savings, damage to reputation, business interruption, downtime costs or any indirect, incidental, consequential, special, punitive, exemplary or any similar type of damages arising out of or in any way related to this DPA or the use or the inability to use Fluxx's products or services, even if advised of the possibility of such damages; and (ii) in no event shall Fluxx's total liability to Customer, its Affiliates and its and their respective officers, directors, employees, agents, customers and representatives for all claims arising out of or as a result of this DPA exceed the greater of \$300,000 USD or the fees paid by Customer to Fluxx in the twelve (12) month period preceding the event giving rise to the liability.

## **11. Miscellaneous**

**11.1 Assignment.** This DPA may not be assigned (whether by operation of Law or otherwise) in whole or in part by either Party without prior consent of the other Party and assurances that all obligations herein will be satisfied, provided however that either Party may assign this DPA in connection with an authorized assignment of the Agreement to the assignee of the Agreement. Any assignment otherwise is in violation of this provision and will be void.

**11.2 Execution of DPA Upon Execution of Order.** This DPA is effective upon the Parties' execution of the Order to which this DPA is attached, and each Party acknowledges and agrees that execution of the Order constitutes execution of this DPA.

**11.3 Governing Law.** This DPA and all claims or causes of action (whether in contract or tort) that may be based upon, arise out of or in any way relates to this DPA, will be governed by and construed in accordance with the Laws identified in the Agreement, except to the extent that Data Protection Laws require otherwise. In such an event, and to the extent so required, this DPA will be governed in accordance with such Data Protection Laws and, if applicable, be subject to the jurisdiction of the relevant data exporter that exported the Personal Data from Europe.

## **Attachment 1 to DPA - The Standard Contractual Clauses**

### **Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Processor Established in a Third Country (Controller-to-Processor Transfers)**

#### **SECTION I**

#### **CLAUSE 1**

##### **Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

#### **CLAUSE 2**

##### **Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### **CLAUSE 3**

#### **Third-party beneficiaries**

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### **CLAUSE 4**

#### **Interpretation**

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### **CLAUSE 5**

#### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### **CLAUSE 6**

#### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

## **CLAUSE 7 - Optional**

### **Docking clause**

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

## **SECTION II - OBLIGATIONS OF THE PARTIES**

### **CLAUSE 8**

#### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

#### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

#### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

#### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

#### **8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of

the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

### **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offenses (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

### **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

### **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## CLAUSE 9

### Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## CLAUSE 10

### Data subject rights

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

## CLAUSE 11

### Redress

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## CLAUSE 12

### Liability

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### **CLAUSE 13**

#### **Supervision**

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the

measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### **CLAUSE 14**

##### **Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination - including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## **CLAUSE 15**

### **Obligations of the data importer in case of access by public authorities**

#### **15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **SECTION IV - FINAL PROVISIONS**

### **CLAUSE 16**

#### **Non-compliance with the Clauses and termination**

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### **CLAUSE 17**

##### **Governing law**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Republic of Ireland.

#### **CLAUSE 18**

##### **Choice of forum and jurisdiction**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of Ireland.
- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

#### **APPENDIX**

##### **ANNEX I**

##### **A. LIST OF PARTIES**

**Data exporter(s):** [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Name: .

Address: .

Contact person's name, position and contact details: .

Activities relevant to the data transferred under these Clauses: .

Signature and date: .

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**Data importer(s):** [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

1. Name: Fluxx Labs, Inc.

Address: .

Contact person's name, position and contact details: .

Activities relevant to the data transferred under these Clauses: Provision of Services as defined by the Agreement.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

Role (controller/processor): Processor

**B. DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Registered users of Customer.

Categories of personal data transferred

Name, email addresses, addresses, phone numbers, financial information, and other categories of Personal Data provided by Customer.Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None.The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Ongoing.Nature of the processing

Provision of Services as defined by the Agreement.Purpose(s) of the data transfer and further processing

To authenticate an authorized user, create an account, and grant the user access to and use of the Services; to assess usage and secure the Services; and to provide technical and customer support.The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal Data will be retained for the Term of the Agreement.For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described in Annex III.

## ANNEX II

### TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

#### 1. FRAMEWORK

The Data Importer has put in place a variety of technical and organisational security measures to protect Personal Data which are implemented and managed by the data privacy and information security leaders in the Data Importer.

#### 2. POLICIES

The Data Importer is subject to data security requirements set forth in its policies, procedures, standards and guidelines that define various aspects of required protection for personal data, including (data importer to tick as appropriate):

- Information Security Policy;
- Computer and Network Security Policy;
- Data Classification Policy;
- Document Management Policy; and
- IT Infrastructure Physical Security Policy.

#### 3. STAFF EDUCATION, TRAINING AND RESPONSIBILITIES

The Data Importer provides data privacy and information security education for all relevant employees upon hire and at least annually so that they understand their responsibilities for safeguarding Personal Data.

#### 4. INCIDENT MANAGEMENT

The Data Importer maintains documented:

- Business Continuity,
- Disaster Recovery, and,
- Incident Response policies and procedures to respond to, and document responses to, relevant disruptions and events.

The Data Importer performs testing of these procedures and provides education to relevant staff at least annually.

#### 5. USER ACCESS TO INFORMATION SYSTEMS

The Data Importer maintains:

- password-based,
- badge-based, and/or
- multi-factor authentication mechanisms for access to all sensitive data, systems, or physical assets.

The Data Importer employs role-based access controls and grants the least privilege necessary for job function.

#### 6. PHYSICAL ACCESS CONTROL

The Data Importer maintains badge-based and role-based physical access controls for all offices and data center locations that house sensitive information. The Data Importer maintains role-based access controls and full-disk encryption on portable IT assets such as laptops.

#### 7. IT SYSTEM SECURITY

It is the Data Importer's policy that business units implement various controls, processes and standards for safeguarding IT systems, which may include:

- controls for the prevention, detection and removal of malicious code, including malware, using approved automated and manual monitoring solutions and countermeasures;
- processes for identification of technical vulnerabilities and resolution where identified;
- minimum security requirements in network services agreements;
- standards for audit trails / logs that record system administrator activity, significant exceptions and information security events;
- processes for monitoring key systems for potentially unusual or suspicious activity and investigating exceptions;
- processes for the timely reporting of information security events or suspected security weaknesses and the development and execution of corrective action plans;
- system access controls that include user authentication, use of unique identifiers (user ID) and, for remote access, two-factor authentication; and
- procedures to control the installation of software on operational systems.

#### 8. **DATA LEAKAGE/MEDIA HANDLING/CRYPTOGRAPHIC CONTROLS**

The Data Importer maintains:

- a Data Classification Policy which defines acceptable use and required protection mechanisms for various types of sensitive data.

The Data Importer employs:

- data encryption,
- role-based access controls,
- network segmentation via firewalls,
- log/event monitoring, and
- automated 24/7 incident alerting to minimize the risk of data leakage.

#### 9. **THIRD PARTY SERVICE PROVIDERS**

The Data Importer vets all third-party service providers to ensure that the processing of data by such providers meets the Data Importer's Company security guidelines. Third party service providers are subject to agreements governing the handling and processing of personal data on behalf of the Data Importer.

#### 10. **STORAGE OF PERSONAL DATA**

Personal Data is to be kept only for as long as is necessary in accordance with the Data Importer's Data Policy and relevant local laws and regulations.

#### 11. **DISPOSAL OF PERSONAL DATA**

When Personal Data is no longer required for business, legal or regulatory obligations, the Data Importer securely destroys the data. Hard-copy materials are destroyed by: cross-cut shredding, pulping, incineration or other methods with reasonable assurance that the material cannot be reconstructed. Sensitive data on electronic media must be rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).

**ANNEX III****LIST OF SUB-PROCESSORS**

## EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorization of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

<b>Vendor Name</b>	<b>Address</b>	<b>Contact Person Name</b>	<b>Contact Person Position</b>	<b>Contact Details</b>
Airbrake	98 San Jacinto Blvd, Suite 1300, Austin, TX 78701	Stuart Moore	Sales Engineer	sales@airbrake.io
AWS*	410 Terry Avenue N, Seattle, WA 98109 United States	Scott Lawson	Senior Account Executive & Team Lead	lawss@amazon.com
Domo	772 East Utah Valley Drive, American Fork, UT 84003	Chris Sink		Chris.Sink@domo.com
Google* (Gsuite)	1600 Amphitheatre Parkway Mountain View, CA 94043	Kim Horwitz	Customer Success Manager	Khorwitz@rippling.com
Microsoft* Azure	1 Microsoft Way. Redmond WA 98052-6399		Support	<a href="https://support.microsoft.com/en-us/topic/contact-microsoft-azure-support-2315e669-8b1f-493b-5fb1-d88a8736ffe4">https://support.microsoft.com/en-us/topic/contact-microsoft-azure-support-2315e669-8b1f-493b-5fb1-d88a8736ffe4</a>
Pendo	418 South Dawson Street Raleigh, NC 27601	Brian Coules	Corporate Account Executive	brian.coules@pendo.io
RackSpace	1 Fanatical Pl. City of Windcrest San Antonio, TX 78218			

Rapid7	Logentries (JLizard Ltd.), Dogpatch Labs, 35 Barrow St., Dublin, Ireland			
Workato	215 Castro St, Ste. 300, Mountain View CA 94041	Richy Mulcahy	Embedded Customer Success Manager	richy.mulcahy@workato.com
Zipdev	3111 Camino del Rfo N San Diego, CA 92108	Daniel Altenburg	Co-Founder	dra@zipdev.com

\*Customer acknowledges and agrees that certain Subprocessors provide services only pursuant to such Subprocessor's standard terms and conditions without negotiation and that such standard agreement(s) are hereby deemed to meet the privacy, confidentiality, security and data protection obligations required by this DPA.

# Fluxx Labs Privacy Notice

Last updated: May 9, 2019

Fluxx Labs Inc. (collectively, "Fluxx", "we" or "us") provides a hosted grant management software platform ("Services") as part of its core mission to connect grantmakers and foundations with grantseekers. In order to provide our Services, we collect and process personal information. This Privacy Notice ("Privacy Notice") is intended to help you better understand how we process your personal information, and governs how Fluxx may collect, use, store and disclose personal information that we obtain through or from:

- Visitors to [www.fluxx.io](http://www.fluxx.io) ("Site") and our mobile application ("Application");
- Grantmakers ("Grantmaker") and grantseekers ("Grantseeker") who register to use our Services;
- Individuals who register for our marketing or corporate events (such as webinars), or sign up to receive our marketing materials, whitepapers or demos;
- Individual sites hosted by Grantmakers via Fluxx with a URL in the <client>.fluxx.io format ("Grantmaker Sites");
- Data submitted by individuals directly to the Grantmaker Sites and that we process on behalf of Grantmakers;
- Your direct communications with us;
- Grantseeker accounts and websites ("Grantseeker Platform"); and
- Publicly available sources and some of our partners.

When we refer to the "Platform" throughout this Privacy Notice, we mean the Site, our Application, Grantseeker Platform, and any other websites, products, software, applications, content, data feeds and other services on which an authorized link to this Privacy Notice is posted.

We recommend that you read this Privacy Notice carefully as it provides important information about your personal data. It also tells you about your rights under the law may protect you.

By accessing or using the Platform and our Services, or submitting information through the Platform, you acknowledge and agree that you have read, understand, and agree to the terms of this Privacy Notice and agree to the collection, use, and disclosure of your personal information in accordance with this Privacy Notice.

IF YOU DO NOT AGREE WITH OUR POLICIES AND PRACTICES, UNLESS OTHERWISE STATED, YOUR CHOICE IS NOT TO USE OR ACCESS THE PLATFORM.

This Privacy Notice is designed so that you can easily reach the section that you are interested in.

If you have any questions, comments, or concerns regarding this Privacy Notice and/or our data practices, or would like to exercise your rights, do not hesitate to contact us. See [How to Contact Us About Privacy](#) and [Additional Legal Rights For Users in the Euro:2ean Economic Area](#) below.

## **1. Who We Are**

Depending on the context in which you provide personal information while visiting or using the Platform, Fluxx may be the data controller or data processor of your personal information under this Privacy Notice. When Fluxx acts as data controller, we are responsible for determining how and why we collect, process or disclose the personal data collected by us or on our behalf. Fluxx is a data controller with respect to visitors to and users of the Site, which, for the avoidance of doubt, includes those users accessing the Platform and/or Services as Grantseekers and Grantmakers. When Fluxx acts as a data processor, Fluxx processes data submitted to Fluxx on behalf of or at the direction of a separate individual or entity. Fluxx is a data processor with respect to personal information submitted by individuals to the Grantmaker Sites, and processes such data on behalf of or at the direction of Grantmakers, as further explained [here](#).

You can Contact Fluxx at: [i:2rivacy@fluxxlabs.com](mailto:i:2rivacy@fluxxlabs.com)

or

Fluxx Labs, Inc.  
2261 Market Street, #4060  
San Francisco, CA 94114  
United States of America

## **2. What Personal Information Do We Collect and How Is It Collected?**

Personal data, or personal information, means any information about an individual from which that person may be identified. For example, it may include your name, telephone number, email address, or payment information, and in some jurisdictions your IP address. It does not include data from which the identity of an individual has been definitively removed along with any identifiers connected to such individual (also known as anonymous or anonymized data).

How we collect personal information directly from you depends on how and why you use the Platform. For instance, the information that you provide when you visit our Site and download a whitepaper or request a demo is more limited than the information you provide if you have registered to use the Platform and our Services as a Grantmaker or Grantseeker.

Individuals may be given the opportunity, by invitation, to submit information directly on a Grantmaker Site (collectively, "Grantmaker Site Users"). If you are a Grantmaker Site User, please be advised that Grantmakers determine the personal data that they collect from you, and this information is stored and processed on the Platform by Fluxx as a data processor. See [Information We Process on Behalf of Grantmakers](#) below.

With respect to the data that Fluxx collects directly, we have divided this Section into three parts in order to better explain the circumstances where personal information may be collected, as well as the types of data collected:

1. Information From Site Visitors
2. Information From Grantmakers
3. Information From Grantseekers

Please be advised that we may ask you to update your information from time to time in order to keep it accurate. Additionally, if you provide personal data to us about someone else, you must ensure that you are entitled to disclose that information to us and that, without us taking any further steps required by data protection laws, we may collect, use and disclose such information for the purposes described in this Privacy Notice. For example, you should ensure the individual concerned is aware of the terms detailed in this Privacy Notice.

#### ***i. Information from Site Visitors***

When you visit the Site or Grantseeker Platform, and depending on the purpose of your visit, you may provide us with personal information if you:

- Create an account;
- Download a whitepaper or sign up for a webinar;
- Request a demo;
- Request marketing materials; and/or
- Communicate with us directly.

In connection with the above-mentioned activities, Fluxx collects the following information:

- Your identity (including your first name, last name, company name);
- Your job title;
- Your email address or other contact information;
- Other information that you may provide by filling out forms or by contacting us (including your feedback or other communications with us).

n some cases, you will not provide any information to us directly, in which case the only data that we collect is Device Information, as explained below.

**ii. Information From Grantmakers**

As an individual Grantmaker, or when you act on behalf of a Grantmaker organization, you provide us with personal information when you:

- Create an account on the Platform;
- Sign up for our Services;
- Create a Grantmaker Site; and/or
- Communicate with us directly.

In connection with the above-mentioned activities, Fluxx collects the following information:

- Your identity, including your first name, last name, organization name);
- Your job title;
- Your password and user name;
- Your contact details, including your postal address or your organization's postal address, email address, phone number(s);
- Your preferences;
- Other information you may provide by filling out forms or by contacting us (including your feedback or other communications with us).

**iii. Information From Grantseekers**

If you are a Grantseeker, we collect and process personal information when you:

- Create an account via the Platform;
- Sign up for our Services;
- Use and interact with the Platform and/or a Grantmaker Site; and/or
- Communicate with us directly.

In connection with the above-mentioned activities, Fluxx collects the following information:

- Your identity: first name, last name, organization name;
- Your password and user name;
- Your contact details: postal address (or address of your organization), email address, phone numbers);
- Your job title (if applicable).
- Your preferences;
- Information about your transactions with Fluxx - this only includes partial payment or credit card information, which is processed and stored exclusively by Stripe, our third-party payment processor;
- Other information you may provide by filling out forms or by contacting us (including your feedback or other communications with us).

### **3 Information We Process on Behalf of Grantmakers**

For Grantmakers, Fluxx hosts individual Grantmaker Sites that enable Grantmakers to manage their grants, projects, and relationships, and depending on the level of service for which each individual Grantmaker registers, budgeting and compliance. With respect to personal information collected by Grantmakers via their individual Grantmaker Sites, Fluxx acts as a data processor. To the extent that Fluxx processes personal data on behalf of Grantmakers, it does so for the purposes expressly set forth in this Section 3, and the personal data is handled in compliance with this Privacy Notice.

#### Data Collected by Grantmakers

We require all Grantmakers to post a conspicuous Privacy Notice on the Grantmaker's Site that is compliance with applicable laws, rules and regulations (including, without limitation all applicable data protection laws) and discloses the Grantmaker's collection, use, and processing of personal information. While each Grantmaker controls the nature, type and purpose of the data to be processed via their respective Grantmaker Sites, generally, if you are a Grantmaker Site User, Grantmakers collect the following basic information on Grantmaker Sites:

- Your identity: first name, last name, organization name;
- Your password and user name (which are stored by Fluxx in encrypted form only for the purpose of enabling you to reset your password);

- Your contact details: postal address (or your organization's postal address), email address, phone number(s); and
- Your job title (if applicable).

In addition, Grantmakers, as data controllers, collect from Grantmaker Site Users a variety of additional information as determined exclusively by each Grantmaker on their respective Grantmaker Sites. This nature of the information collected is determined by each individual Grantmaker - based on each such Grantmaker's mission - and is then electronically submitted to the Fluxx Platform for hosting of the Grantmaker Site, indexing and related processing by Fluxx. Although Fluxx processes the personal information of Grantmaker Site Users because it hosts the Grantmaker Sites, it only does so on behalf of Grantmakers, who control the nature, type and purpose of the data to be processed via their respective Grantmaker Sites. In other words, Grantmakers choose what information they collect from Grantmaker Site Users, and Fluxx processes personal data only as provided in its individual agreements with Grantmakers

#### Use and Disclosure

If you submit personal information to a Grantmaker Site, please check with the Grantmaker directly about the policies and settings it has in place with respect to how it handles privacy and security of the personal information that you submit directly in connection with your use of the Grantmaker Site.

Fluxx's processing of personal information collected by Grantmakers on their respective Grantmaker Sites is limited to the purpose of providing the Services to the Grantmakers. However, to the extent that Fluxx processes personal data that it receives from Grantmaker Site Users, it does so for the purposes expressly set forth in this Section 3 and in compliance with this Privacy Notice.

With respect to disclosure of personal information, Fluxx and Grantmakers may process your personal information with the assistance of third-party service providers, as explained [here](#).

#### Contacting Grantmakers and Exercising Legal Rights

Fluxx has no direct relationship with Grantmaker Site Users to the extent that their personal information is hosted or transmitted through the Grantmaker Sites. Grantmakers are responsible for complying with any regulations or laws that require providing notice, disclosure, and/or obtaining consent prior to transferring the data to Fluxx for processing purposes.

If you have are a Grantmaker Site User and have any questions about your personal information, please contact the relevant Grantmaker. In addition, for Grantmaker Site Users located in the European Economic Area, requests regarding personal data must first be addressed to the Grantmaker directly, and as a processor, Fluxx will assist in handling such requests, as explained below in Additional Legal Rights For Users in the EuroRean Economic Area. As data controllers, Grantmakers have the ability to fulfill these requests, and Fluxx will provide assistance for requests that Grantmakers are not able to complete. If you request that Fluxx remove your personal information, we will refer your request to the applicable Grantmaker and respond to the request within 30 days.

You may also report concerns with personal information hosted or transmitted at the direction of Grantmakers by contacting us at Rrivacy\_@fluxxlabs.com. We will refer your requests to the appropriate Grantmaker.

#### **4. Information Collected Indirectly**

##### *Device Information*

When you use or interact with the Platform or the Grantmaker Sites, even if you do not have an account, we, or our authorized third-party service providers, automatically collect information about the Services you use and how you use them via your device (collectively, "Device Information"). We use this information for our internal purposes, specifically to operate, maintain, secure and improve the Platform and our Services.

Device Information that we collect consists of:

- **Usage Information.** We automatically collect information about your interactions with the Platform and Grantmaker Sites, including your information about your device: IP address, access dates and times, information about your approximate location (as determined through your IP address), hardware and software information, device information, device event information, crash data, cookie data. This information allows Fluxx to understand the pages or content you view, your searches, how you've used the Services (which may include administrative and support communications with us or whether you have clicked on third- party links), and other actions on the Platform and Grantmaker Sites. We automatically collect log data when you access and use the Platform, even if you have not created an account or logged in. We use this information for our internal purposes only and to improve the Platform, our Grantmaker Sites and our Services.
- **Cookies and Similar Technologies.** We or authorized third parties collect certain information by automated means using cookies, web beacons, and server logs for analytic purposes. The information we collect in this manner enables is to better understand website traffic patterns and to optimize user experience. For instance, through Google Analytics, we are able to detect your "referral address." We do not, however, use cookies or similar technologies to actively track users across other websites. For more information on our use of these technologies, see our Cookie Policy.

### *Aggregated Data*

With the Device Information collected by our third-party analytics services, we process, "Aggregated Data", such as statistical or demographic data. Aggregated Data may be derived from personal data, but is not considered personal data under the law if it does not directly or indirectly reveal your identity. For example, we may aggregate usage data to calculate the percentage of users accessing a specific feature of our Platform or the Grantmaker Sites. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data, which will be processed in accordance with this Privacy Notice.

To opt out of the collection of Device Information by Google Analytics or Mixpanel, please see [Managing Your Preferences](#) below.

### *Information from Third Parties*

In some instances, we process personal information from third parties, which consists of:

- Data from publicly-available sources, such as public records that are available online; and
- Data from our partners, such as transactional data from providers of payment services.

## **5. Sensitive Data**

Fluxx does not (and does not want to) collect any sensitive data that includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic, and biometric data. Pursuant to individual agreements and Terms of Service, Grantseekers and Grantmakers may only collect sensitive information in accordance with applicable law, which may include valid consent from individuals. If you believe that your sensitive information has been collected or otherwise processed by a Grantmaker or Grantseeker, please notify Fluxx and the relevant Grantmaker or Grantseeker.

## **6. Children's Privacy**

Neither our Platform and the Grantmaker Sites, nor our Services, are intended for minors. Fluxx does not target its Services to persons under the age of 18 and does not knowingly collect personal data from minors. Therefore, we ask you not to provide us with personal information of persons under the age of 18. If we learn that personal information of persons under 18 years of age has been collected on or through the Platform or the Grantmaker Sites, then we may deactivate the account and/or make the user content inaccessible, or direct our Grantmakers to do the same.

## 7. Why We Collect Your Personal Information and How We Use It

Our mission is to provide a safe, efficient and high-quality Platform, and we, or our authorized third party service providers who assist us in providing the Services, process your personal information for this purpose. Personal information may generally be processed for the following reasons:

- In order to perform services under a contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party), and your interests and fundamental rights do not override those interests.
- Where necessary to comply with a legal or regulatory obligation.
- If we have obtained your prior consent. Please note that for this specific legal basis, you have the right to withdraw your consent at any time.

More specifically, and depending on how you use our Services, Fluxx processes your personal data in the following instances and in order to:

- Provide you with our Services - providing webinars, demos, and the Grantseeker Platform, as well as hosting Grantmaker Sites (performance of a contract or sometimes necessary for our legitimate interests, depending upon the circumstances);
- Enable Grantseekers to connect with Grantmakers (performance of a contract);
- Conduct checks to verify identity (performance of a contract or sometimes necessary for our legitimate interests, depending upon the circumstances);
- Send you direct marketing communications regarding Fluxx's products and services that we may think are of interest to you (with your prior consent where you are not an existing customer);
- Respond to your queries and requests, or otherwise communicate directly with you (performance of a contract or sometimes necessary for our legitimate interests, depending upon the circumstances);
- Detect any fraudulent or illegal activity against you and/or Fluxx (necessary for our legitimate interests);

- Perform system maintenance and upgrades, and enable new features (performance of a contract or sometimes necessary for our legitimate interests, depending upon the circumstances);
- Conduct statistical analyses (necessary for our legitimate interests);
- Provide information to regulatory bodies when legally required, and only as outlined below in Section 10(.) of this Privacy Notice (necessary for compliance with a legal obligation).

## **8. Marketing Communications**

If you are an existing customer, and have not otherwise opted out, or if you have opted in to receive direct marketing emails from us, we may use your personal information to send you marketing information. For instance, when you request a demo or download a whitepaper, you will be asked if you wish to opt in to receive marketing communications from us for our products and services. This is what we call direct marketing. We carry out direct marketing by email.

Unless you are an existing customer or a prospective customer, we rely on your consent to process the personal data you provide to us for this purpose. In either case, if you no longer wish to receive such information, you have the right at any time to opt out of marketing emails and withdraw your consent at any time. The easiest way to opt out is to use the unsubscribe link that you will find at the bottom of each communication. You may also manage your preferences as further explained in

[Managing Your Preferences.](#)

## **9. Managing Your Preferences**

### *Direct Marketing*

As explained above, Fluxx enables you to manage your marketing preferences by clicking on a link contained in each electronic communication to you. Please use your preference settings to inform us of how you would like to receive marketing communications. Updates to your privacy preference information will be submitted once you have confirmed your changes.

Outside the Platform, you may also manage your cookie and tracking preferences as follows:

- Turning off cookies in the preferences settings in your browser. For more information or additional guidance, please click [here](#);
- Downloading the Google Analytics opt-out browser add-on [here](#);
- Fluxx, like many other companies, does not currently respond to Do Not Track ("ONT") signals. Fluxx does not respond to ONT signals in order to provide the Services, maintain security and prevent fraud. For more information on ONT settings generally, please visit <http://allaboutdnt.com>.

## 10. Disclosure of Your Personal Information

Regardless of how you use the Platform, we never sell or rent your personal data, and only disclose it to authorized third parties to the extent strictly necessary, as explained in this section.

Aside from disclosing your information to those of our employees who are authorized to process the information in order to provide our Services and are committed to confidentiality, we disclose your personal information only to the third parties indicated below (and for the following reasons):

- **Companies that do things to help us provide the Services: hosting service providers, user engagement and customer support providers, payment service providers, conference organizers, communication tools, and analytics tools;**
- Professional service providers, such as auditors, lawyers, consultants, accountants and insurers;
- Governments, regulators, law enforcement and fraud prevention agencies, but only as authorized as explained in [Section 1O\(c\)](#). of this Privacy Notice;
- Grantmakers, if you are a Grantseeker and choose to link your information uploaded in the Grantseeker Platform directly to a Grantmaker;
- In the event of a business transfer; and
- Companies approved by you, such as financial institutions or payment service providers.

#### a. Third-Party Service Providers

Specifically, depending on how you use the Platform, the following third parties collect data on our behalf or receive your personal data in order to assist us in providing our Services:

- Amazon Web Services and Google Cloud to host our Platform;
- Google Analytics, New Relic and Mixpanel, to perform analytics on the Platform;
- Hubspot, which provides all of the functionality for the Site (with the exception of the Grantmaker Sites);
- Salesforce, which assists in keeping track of our current and any prospective customers;
- Stripe, a subscription and payment service provider;
- Sendgrid, which sends emails on our behalf;
- Captera and Adwords, to advertise our Platform on other websites;
- LogEntries, to provide centralized log keeping;
- Appcues, to provide help within Grantseeker;
  
- Wistia, which enables us to play videos (for demos and marketing purposes) on our Site.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions, unless the data is rendered fully anonymous.

In addition, our Services for Grantmakers consist of hosting Grantmaker Sites within which Grantmakers may elect to enable or integrate additional services or applications from third parties, including:

- **Lexis Nexis Bridger, which assists Grantmakers with Office of Foreign Asset Score ("OFAC") checks: a Grantmaker may have a separate contract and paid account with Lexis Nexis Bridger (linked to its Grantmaker Site), which enables the Grantmaker to receive and store name, address, phone number, and OFAC score when an OFAC check is done;**
- **Zendesk, for customer support, which may be integrated Grantmakers and enable their administrators to log support tickets, communicate with support, and troubleshoot issues using the Zendesk web portal; and**

- **Google Docs (part of Google Apps), which can be enabled 1n Grantmaker Sites for document editing and previews at Grantmakers' discretion.**

Where Fluxx processes data collected by Grantmakers via third-party integrated services, it processes any and all personal data only for the purpose of providing the Services to Grantmakers as explained in Section 3 and in compliance with this Privacy Notice. Fluxx also remains responsible for the processing of personal information it receives from Grantmaker Sites, and subsequently transfers to a third-party acting as an agent on its behalf. When Fluxx uses third-party service providers, contractors, and sub-processors to assist in providing the Services (including hosting Grantmaker Sites), Fluxx maintains contracts with these third parties that restrict their access, use, and disclosure of personal information.

**b. Business Transfers**

We may also share data with third parties to whom we choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this Privacy Notice or as updated.

**c. Legal Obligations and Security**

**While Fluxx endeavors to provide the highest level of protection for your information, we will preserve or disclose your personal information in limited circumstances, including: (i) with your consent; (ii) when we have a good faith belief it is required by law, such as pursuant to a subpoena, warrant or other judicial or administrative order (as further explained below); (iii) to protect the safety of any person; to protect the safety or security of our Platform or to prevent spam, abuse, or other malicious activity of actors on our Platform; or (iv) to protect our rights or property or the rights or property of those who use our Services.**

If we are required to disclose personal information by law, such as pursuant to a subpoena, warrant or other judicial or administrative order, our policy is to respond to requests that are properly issued by law enforcement within the United States, Canada, Ireland or Australia, or otherwise via mutual legal assistance treaty. Under such circumstances, we will attempt to provide you with prior notice that a request for your information has been made in order to give you an opportunity to object to the disclosure. We will attempt to provide this notice by email, if you have given us an email address. However, government requests may include a court-granted non-disclosure order, which prohibits us from giving notice to the affected individual. In cases where we receive a non-disclosure order, we notify the user when it has expired or once we are authorized to do so.

With respect to any valid legal process (subpoena, warrant or court order) concerning Grantmaker Site Users' or personal information uploaded to the Platform by Grantseekers, any such request will be immediately directed to the Grantmaker or Grantseeker unless we are prohibited from doing so due to a court-granted non-disclosure order. If we are prohibited from providing Grantmakers or Grantseekers with prior notice of such requests, we will notify them of such request after the prohibition has expired, or once we are authorized to do so.

Note that if we receive information that provides us with a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, we may provide information to law enforcement trying to prevent or mitigate the danger (if we have it), to be determined on a case-by-case basis.

**d. Disclosure of Information Between Grantmakers and Grantseekers**

If you are a Grantseeker, you have the option of linking information that you have uploaded to the Grantseeker Platform to Grantmakers directly. If you do so, only the information that you choose to share will be visible to the specific Grantmaker(s) with whom you have connected. Please check Grantmakers' individual policies to determine how they handle and protect personal data.

## **11. Payment Processing**

We do not directly collect your payment information and we do not store your payment information. We use Stripe, a third-party, PCI-compliant, payment processor, which collects payment information on our behalf in order to complete transactions. While our administrators are able to view and track actual transactions via the Stripe customer portal, with the exception of the last 4 digits of your credit card, credit card type, zip code and expiration date, we do not have access to or process your credit card information. Please review Stripe's [Privacy Policy](#) to learn more about how Stripe collects, processes and protects your personal information.

## **12. Third Party Links**

On the Platform, we may provide, for informational purposes only, links to other websites or resources with which we do not have a contractual relationship and over which we do not have control ("External Websites"). Note that Grantmakers may also separately elect to add external links to External Websites in the Grantmaker Sites. Such links are not paid advertisements, nor do they constitute an endorsement by Fluxx of those External Websites, and are provided to you only as a convenience. By clicking on links to External Websites, the operators of the External Websites may collect your personal information. We are not responsible for the content or data collection practices of those External Websites, and your use of External Websites is subject to their respective terms of use and privacy policies.

## **13. Third Party Social Plugins**

On the Site and Grantseeker Platform, we provide third-party "share" buttons for YouTube, Facebook, Twitter or other social media sites, which may function as web beacons when you interact with the button. For instance, we provide a YouTube "share" button for sharing Fluxx's training and new release webinars. As a result of this, please note that you may send to the third party the information that you are viewing on a certain part of the Platform when you "share". If you are not logged into your account with the third party, then the third party may not know your identity. If you are logged in to your account with the third party, then the third party may be able to link information or actions about your interactions with the Platform to your account with them. Please refer to each third party's privacy policies to learn more about its data practices, as also explained in our Cookie Policy

## 14. How Long Do We Keep Your Personal Information?

Your personal information is processed for the period necessary to fulfill the purposes for which it is collected, to comply with legal and regulatory obligations and for the duration of any period necessary to establish, exercise or defend any legal rights.

In order to determine the most appropriate retention periods for your personal information, we consider the amount, nature and sensitivity of your information, the reasons for which we collect and process your personal data, and applicable legal requirements. For example:

- **With regard to Fluxx's users, as well as data collected by Grantmakers from Grantmaker Site Users: personal data is stored for the duration of the commercial relationship and then retained only as required to satisfy applicable contractual, legal and financial retention obligations, after which it is deleted or archived (only if necessary to comply with legal retention obligations for the latter);**
- **Grantmaker and Grantseeker logs, including Device Information, are stored for 12 months to comply with contractual and security requirements.**

In some circumstances, you can ask us to delete your data. See [Additional Legal Rights For Users in the European Economic Area](#) below for further information.

Some exceptions from static retention periods may occur. For instance, we cannot delete personal data when there are legal obligations to retain it (e.g. arising from tax or commercial law). This is particularly true of financial data and payment information. Additionally, we cannot delete personal data when it is needed for the establishment, exercise or defense of legal claims ("litigation hold"). In this case, the personal data can be retained as long as needed for exercising respective potential legal claims.

In some instances, we may choose to anonymize your personal data instead of deleting it, for statistical use, for instance. When we choose to anonymize, we make sure that there is no way that the personal data can be linked back to you or any specific user.

## **15. Protecting Your Personal Data**

No method of transmission over the Internet, or method of electronic storage, is 100% secure, however we take all steps necessary to securely provide all of our Services, whether on the Platform or the Grantmaker Sites. We have put in place appropriate security measures designed to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. For example, we use encryption, secure socket layer, firewalls, and password protection. In addition, we require two-factor authentication for all employees and contractors who may access your data to provide our Services, and we limit access to those employees, agents, contractors and the third parties who have a business need-to-know.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so. We also require those parties to whom we transfer your personal information to comply with the same.

However, no method of transmission over the Internet, or method of electronic storage, is 100% secure, and while we take all reasonable steps necessary to provide the most secure Services, by using our Services, you understand and assume the risks associated with your activities on the internet.

## **16. International Transfers**

Fluxx is based in the United States and has servers in Canada, Ireland, and Australia. The personal information that we collect are sent to and stored on secure servers located in the United States. Such storage is necessary in order to process the information. Fluxx operates globally and may transfer the personal data that we collect from you to our other offices and/or to the third parties mentioned in the circumstances described above, which may be situated outside of your country or regional area, and may be processed by staff operating outside of your country or regional area. In particular, information provided to us or collected by us likely will be transferred to and processed in the United States by us or our agents and contractors. The data protection laws of the United States or other countries may not be as comprehensive or equivalent to those in your country of residence.

The European Union's General Data Protection Regulation ("GDPR") allows for transfer of personal data from the European Union to a third country in certain situations. By your continued use of the Platform, and agreeing to the terms of use and this Privacy Notice, you agree to the transfer of your information to the United States and to the processing of that

information by Fluxx on servers located in the United States as described in this Privacy Notice. Wherever we transfer your personal data, we will take reasonable steps to ensure that your privacy rights continue to be protected. We may also adopt other means, such as entering into Model Contract Clauses. More information about the Model Contract Clauses is available [here](#).

## **17. Additional Legal Rights For Users in the European Economic Area**

**If the GDPR applies to you because you are in the European Economic Area, you have certain rights in relation to your personal data:**

- The right to be informed - our obligation to inform you that we process your personal data (and that's what we're doing in this Privacy Notice);
- The right of access - your right to request a copy of the personal data we hold about you (also known as a 'data subject access request');
- The right to rectification - your right to request that we correct personal data about you if it is incomplete or inaccurate (though we generally recommend first making any changes in your Account Settings);
- The right to erasure (also known as the 'right to be forgotten') - under certain circumstances, you may ask us to delete the personal data we have about you (unless there's an overriding legal reason we need to keep it);
- The right to restrict processing - your right, under certain circumstances, to ask us to suspend our processing of your personal data;
- The right to data portability - your right to ask us for a copy of your personal data in a common format (for example, a .csv file);
- The right to object - your right to object to us processing your personal data (for example, if you object to us processing your data for direct marketing); and
- Rights in relation to automated decision-making and profiling - our obligation to be transparent about any profiling we do, or any automated decision-making.

These rights are subject to certain rules around when you can exercise them. If you are located in the European Economic Area and wish to exercise any of the rights set out above, please contact us (see [How to Contact Us About Privacy](#)..).

You will not have to pay a fee to access your personal data (or to exercise any of the other rights) unless your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request under those circumstances.

We may need to request specific information from you to help us confirm your identity. This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

We will respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated as required by law.

In addition, if you no longer wish to receive our marketing/promotional information, we remind you that you may withdraw your consent to direct marketing at any time directly from the unsubscribe link included in each electronic marketing message we send to you. If you do so, we will promptly update our databases, and will take all reasonable steps to meet your request at the earliest possible opportunity, but we may continue to contact you to the extent necessary for the purposes of providing our Services.

Finally, you have the right to make a complaint at any time to the supervisory authority for data protection issues in your country of residence. We would, however, appreciate the chance to address your concerns before you approach the supervisory authority, so please contact us first.

If you have any questions about this Privacy Notice, including any requests to exercise your legal rights, please contact us using the details in How to Contact Us About Privacy.. below.

If you are a Grantmaker Site User, please direct any requests or questions to the Grantmaker as explained in Section 3 of this Privacy Notice, and Fluxx will assist the relevant Grantmaker.

## **18. How to Contact Us About Privacy**

If you have any questions about this Privacy Notice, have additional questions, or would like to exercise any of your rights if you are located in the European Economic Area, please contact us at Rrivacy\_@fluxxlabs.com. You may also write us at:

Fluxx Labs, Inc.  
Attention: Data  
Privacy  
2261 Market Street, #4060  
San Francisco, CA 94114  
United States of America

## **19. Changes to this Privacy Notice**

Fluxx may need to update this Privacy Notice from time to time. If so, we will post an updated Privacy Notice on our Platform along with a change notice on the Platform. If we make significant changes, we may also send registered users a notice that this Privacy Notice has been changed. We encourage you to review this Privacy Notice regularly for any changes. Your continued use of the Platform and/or your continued provision of personal data to us after the posting of such notice will be subject to the terms of the then-current Privacy Notice.

## **Fluxx Labs Cookie Policy**

Effective date: May 9, 2019

Fluxx is committed to transparency with respect to its data collection and use practices. This Cookie Policy ("Cookie Policy") explains how we use cookies throughout the Platform and your related choices. Please note that this Cookie Policy is provided as a statement about privacy and Fluxx's use of cookies and similar technologies.

Capitalized terms used in this Cookie Policy but not defined herein will have the meanings given to them in Fluxx's Privacy Notice.

### **"COOKIES" EXPLAINED AND WHY THEY ARE USED**

A cookie is a small piece of data (text file) that a website - when visited by a user - asks your browser to store on your computer or device in order to remember information about you, such as your language and/or currency preference or login information. Fluxx may use similar techniques

- web beacons, specifically - which we will refer to collectively as "cookies".

Cookies may be used for many different purposes. For example, cookies can be used to show that you have previously visited the Platform and to identify which parts of the Platform you might be most interested in. Cookies can also improve your online experience by storing your preferences during your visit to the Platform.

#### *Types of Cookies Used by Fluxx*

Fluxx places its own (direct or "first-party" cookies), We also use third-party cookies on the Platform - which are cookies placed by external domains and companies. Cookies and other tracking technologies fulfill the following purposes:

- Assisting you in navigation of the Platform.
- Analyzing your use of the Platform and Services.
- Filling out contact, support and feedback forms.
- Sharing content on the Platform through social media via "share" buttons.

Below is an explanation of the types of cookies that may be used on or through the Platform and why we use them. We classify cookies in the following categories:

- Strictly Necessary Cookies
- Performance Cookies
- Content Sharing Cookies

Where required by applicable law, we will obtain your consent prior to setting cookies (except for strictly necessary cookies). In order to manage your cookie preferences, you may alter the cookie settings in your browser settings at any time. You may accept all, or certain, cookies. If you do disable our cookies in your browser settings, you may find that certain sections of Platform will not work. For example, you may have difficulties logging in.

### **STRICTLY NECESSARY COOKIES - PROPER FUNCTIONS OF PLATFORM AND FLUXX APP**

These cookies are necessary for the Platform to function and cannot be switched off in our systems. They are usually only set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in or filling in forms. You can set your browser to block or alert you about these cookies, but some parts of the Platform may not work.

Fluxx and its third-party service providers (as set forth in the Privacy Notice) use these cookies to:

- Remember information that you fill in when performing certain activities on the Platform.
- Pass information from one page to the next, for example when filling out support forms or surveys.
- Store your preferences such as language, location, and currency.

- Store settings for optimal video display, such as buffer size and your computer or devices resolution details.
- Read your browser and device settings to optimize the display of the Platform.
- Locate and identify misuse of the Services.
- Load the Platform uniformly to maintain accessibility.
- Offer options to store your log-in details to streamline your access to the Platform and Services.
- Enable embedded video content.
- Fraud prevention and authentication.
- Provide the ability to "like" or "favorite" content on the Platform.

## **PERFORMANCE COOKIES - PLATFORM AND FLUXX APP USAGE ANALYTICS**

These third-party cookies allow us to count visits and traffic sources, so we can measure and improve the performance of the Platform. They help us know which pages are the most and least popular and see how visitors move around the site.

These cookies are used to:

- Keep track of the number of visitors to the pages within the Platform.
- Keep track of the length of time that each visitor spends on the pages within the Platform.
- Determine the order in which a visitor visits the various pages within the Platform.
- Determine the website a visitor was at before navigating to the Platform and the website a visitor is going to immediately after leaving the Platform.
- Identify Platform performance issues.
- Assess which parts of the Platform need improvement.

## CONTENT SHARING COOKIES - SHARING PLATFORM CONTENT VIA SOCIAL MEDIA

Certain content on the Platform (e.g. articles, pictures and videos) can be shared and liked via social media by means of "share" buttons. If you click on the "share" button for a third-party social media site, that social media site will collect your personal information and data for their own purposes. As stated in the Privacy Notice, Fluxx has no control over how these third-party social media services make use of your personal information and data. We encourage you to read the applicable privacy policies for such third-party social media services to understand how your personal information may be used by them - and adjust your privacy settings accordingly. Please refer directly to the privacy policies linked below of the third-party social media services currently available through the Platform:

- [Facebook](#)
- [Twitter](#)
- [YouTube](#) (Google)
- [LinkedIn](#)

## YOUR OPTIONS: MANAGE TRACKING AND OPT OUT

While tracking is widespread over the internet, there are things you can do to minimize these activities, as explained here.

- You may download the Google Analytics opt-out browser add-on [here](#).
- Fluxx, like many other companies, does not currently respond to Do Not Track ("DNT") signals. Fluxx does not respond to DNT signals in order to provide the Services, maintain security and prevent fraud. For more information on DNT settings generally, please visit <https://allaboutdnt.com>.
- With respect to social media "share" buttons, many of these social media sites handle tracking differently depending on whether or not a user is logged in and the preferences selected by users. If you use social media and want to protect your browsing privacy, we recommend that you adjust your individual settings for each third-party social media company with whom you have an account, so as to minimize cross-site tracking.
- To learn more about cookies, including how to manage cookies and opt-out of cookies being placed on your device, please visit <http://www.allaboutcookies.org/manage-cookies/index.html>.

## **CHANGES TO THIS COOKIE POLICY**

Fluxx reserves the right to amend this Cookie Policy and the cookies included in the lists at any time and without notice. The updated and amended Cookie Policy will be effective upon posting. If you do not agree to the revised Cookie Policy, you should alter your preferences, or consider ceasing use of the Platform. By continuing to access or make use of the Platform and our Services after the changes become effective, you agree to be bound by the revised Cookie Policy.

If you have any questions and/or comments regarding this Cookie Policy, please contact us [Rrivacy@fluxxlabs.com](mailto:Rrivacy@fluxxlabs.com).