Data Processing Addendum

This Data Processing Addendum ("**Addendum**") supplements the FloQast Close Management Software Services Agreement (the "**Agreement**") entered into by and between the applicable FloQast, Inc. customer ("**Controller**") and FloQast, Inc. ("**Processor**" or "FloQast") (each a "**Party**" and collectively the "**Parties**"). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

1. Definitions

1.1 "**Applicable Law(s)**" means any state, federal or foreign law(s), rule(s) or regulation(s) applicable to the Addendum, the Agreement, or the Processing, including those concerning privacy, data protection, confidentiality, information security, availability and integrity, or the handling or processing of Personal Data. Applicable Laws expressly include, if applicable, CCPA (as defined below , the United Kingdom Data Protection Act 2018 (the "**UK Data Protection Act**"), United Kingdom's Privacy and Electronic Communications Regulations 2003 (as amended), including any superseding regulation, , the General Data Protection Regulation (Regulation (EU) 2016/679) (the "**GDPR**"), GDPR as transposed into United Kingdom national law by the operation of section 3 of the EU (Withdrawal) Act 2018 (and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) (the "**UK GDPR**"), EU Directive 2002/58/EC (the "**ePrivacy Directive**"), and, when effective, any regulation expressly superseding the ePrivacy Directive, as well as the laws, rules, and regulations of each nation in the European Economic Area ("**Member State Law(s)**" and the United Kingdom.

1.2 "**Authorized Employee**" means an employee of Processor or a Processor Affiliate who has a need to know or otherwise access Personal Data in order to enable Processor to perform its obligations under this Addendum or the Agreement and who has undergone appropriate background screening and training by Processor.

1.3 "**Authorized Person**" means an Authorized Employee or Authorized Subprocessor.

1.4 "**Authorized Subprocessor**" means a third-party subcontractor, agent, reseller, or auditor engaged by Processor, or employee of same, that has a need to know or otherwise access Personal Data to enable Processor to perform its obligations under this Addendum or the Agreement and that has been previously approved by Controller in writing to do so, and who is bound in writing by a data processing agreement which is compliant with GDPR and/or the UK GDPR and/or CCPA pursuant to which their duties and obligations to protect Personal Data are in strict accordance with the terms hereof.

1.5 "**California Consumer Privacy Act of 2018**" or "**CCPA**" means Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the California Civil Code, including all amendments thereto.

1.1 "**Controller Affiliate**" means any entity that owns or controls, is owned or controlled by, or is under common control or ownership with Controller (where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether by contract, exercise of voting rights, common management, or otherwise).

1.6 "**Data Subject**" means an identified or identifiable person to whom Personal Data relates who is in the EEA or the United Kingdom or whose rights are protected by GDPR or the UK GDPR or (ii) a "Consumer" as the term is defined in the CCPA.

1.7 "**Data Subject Rights**" means the rights recognized and granted to Data Subjects with respect to their Personal Data under Applicable Laws, including, the GDPR or the UK GDPR (as set forth in Articles 12 through 22 thereof) or as defined in the CCPA

1.8 "**Data Protection Impact Assessment**" or "**DPIA**" means an assessment, conducted pursuant to Controller's Instructions, of the impact of one or more Processing operations on the protection of Personal Data and the privacy of Data Subjects that takes into account the nature, scope, context, and purposes of such Processing and includes, without limitation, an analysis of the necessity and proportionality of such Processing as well as the appropriateness of the Technical and Organizational Measures used in connection with such Processing.

1.9 "**Incident**" means a situation whereby Personal Data in either Processor's or any Authorized Person's systems, backups, networks, servers, databases, computers, or other hardware or technical infrastructure, was lost with a low risk of potential harm or damage to Data Subjects.

1.10 "**Including**" and its derivatives (such as "include" and "includes") (whether or not capitalized) means "including, without limitation" unless expressly indicated otherwise.

1.11 "**Industry Standards**" means the then-current industry best data protection and data processing practices relating to the Processing of the Personal Data.

1.12 "**Instruction**" means a direction issued by Controller to Processor and/or any Authorized Person, documented either in textual form (including without limitation by e-mail) or by using a software or online tool, regarding the Processing of Personal Data.

1.13 "**International Data Transfer**" means any transfer of Personal Data from the EEA, Switzerland or the United Kingdom to an international organization or to a country outside of the EEA, Switzerland and the United Kingdom, and includes any onward transfer of Personal Data from the international organization or the country outside of the EEA, Switzerland or the United Kingdom to another international organization or to another country outside of the EEA, Switzerland and the United Kingdom.

1.14 “**Personal Data**” means any information relating to a Data Subject which Processor: (i) receives from or on behalf of Controller, or the Controller’s Affiliates or (ii) accesses, for Processing in connection with the Services, and includes Sensitive Personal Information.

1.15 “**Personal Data Breach**” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

1.16 “**Process**” or “**Processing**” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, transfer, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.17 “**Processor Affiliate**” means any entity that owns or controls, is owned or controlled by, or is under common control or ownership with Processor (where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether by contract, exercise of voting rights, common management, or otherwise) and that assists or enables Processor to fulfill its obligations under the Agreement and Addendum.

1.18 “**Restricted Transfer**” means a transfer of Personal Data from the European Economic Area, United Kingdom or Switzerland to any country or recipient: (i) not deemed by the European Commission or the UK Information Commissioner's Office as providing an adequate level of protection for Personal Data, and (ii) not covered by or a suitable framework or certification recognized by the relevant Supervisory Authority as providing an adequate level of protection for Personal Data.

1.19 “**Sensitive Personal Information**” means a Data Subject’s (including without limitation a Controller employee’s, where applicable) (i) government-issued identification number (including social security number, driver’s license number or state-issued identification number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual’s financial account; (iii) genetic, biometric or health data; (iv) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or sexual activity, or trade union membership; (iv) Personal Data relating to criminal convictions and offences (including commission of or proceedings for any offense committed or alleged to have been committed) and (v) any other Personal Data designated as sensitive or deserving of heightened protection under applicable United Kingdom or individual Member State Law or the CCPA.

1.20 “**Services**” shall have the meaning set forth in the Agreement.

1.21 “**Standard Contractual Clauses**” means the clauses annexed to EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ L 39, 12.2.2010, p. 5-18), or the UK Information Commissioner's Office, and any successor clause,s as may be approved by Supervisory Authorities from time to time.

1.22 “**Supervisory Authority**” means any other court, tribunal, or governmental or quasi-governmental entity or agency that has jurisdiction, under Applicable Law, over the Agreement or Addendum, the Personal Data or Processing, and/or Controller or Processor, including the United States Department of Commerce and the data protection authorities of the nations of the European Economic Area, United Kingdom and of Switzerland and California.

1.23 “**Technical and Organizational Security Measures**” means the measures taken by Processor and Authorized Persons as set out in Exhibit B, and as may be updated, varied or improved by the Processor from time to time, provided that the Processor shall ensure that any such updates, variations, or improvements provide no less security protection than those set out in Exhibit B. Such measures are aimed at (i) ensuring the confidentiality, security, integrity, and availability of Personal Data, including protecting against an Incident, a Personal Data Breach, or other accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure or access to Personal Data (in particular where Processing involves the transmission of Personal Data over a network) and other unlawful forms of Processing and/or (ii) assisting and enabling Controller to comply with its obligations to respond to requests by Data Subjects to exercise their Data Subject Rights.

2. Processing of Data

1.2 Processor agrees to comply with this Addendum at all times during the term of the Agreement. Any failure by Processor to comply with the obligations set forth in this Addendum, or any Personal Data Breach, will be considered a material breach of the Agreement, and Controller will have the right, without limiting any of the rights or remedies under this Addendum or the Agreement, or at law or in equity, to immediately terminate the Agreement for cause. Processor acknowledges that Controller may be the controller of the Personal Data or may be a processor of the Personal Data on behalf of another controller.

2.1 The rights and obligations of the Controller with respect to Processing are described herein and in the Agreement. The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects involved, are described in Exhibit A to this Addendum.

2.2 Processor acknowledges and agrees that it shall only Process Personal Data for the limited and specified purposes described in Exhibit A and in compliance with the Controller's obligations under the relevant laws, the terms and conditions set forth in this Addendum.

2.3 Subject to Sections 2.5 and 2.6, the Processor shall processes Personal Data only on documented instructions from the Controller which are set out in this Addendum or in the written agreement which the Processor has with the Controller. This includes, without limitation, the instructions set out in this Addendum regarding transfers of personal data to third countries.

2.4 The Processor may process Personal Data other than in accordance with Section 2.4 if required to do so in order to comply with Applicable Law, in which case, the Processor shall inform the Controller of the relevant Applicable Law before is commences such Processing unless such Applicable Law prohibits the Controller from doing so on important grounds of public interest;

1.3 The Processor shall not be required to comply with any instructions which in the opinion of the Processor infringe any Applicable Law in which case, the Processor shall notify the Controller immediately of such applicable law.

1.4 Processor warrants that its Processing of Personal Data does and will comply with all Applicable Laws.

1.5 To the extent that any Personal Data is transmitted, transferred, shared or otherwise disclosed to Processor from any Member State, United Kingdom or Switzerland the Processor warrants that it shall comply with GDPR, UK GDPR and all other Applicable Laws to its business, with respect to any Processing, including in particular any transfer, of such Personal Data.

2. Security of Data

2.5 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons (collectively, "**Risks**"), Processor shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data as set forth on Exhibit B.

2.1 Upon Controller's written request, or, upon the termination or expiration of the Agreement for any reason, Processor shall, and shall ensure that all Authorized Persons, (i) promptly and securely delete (in accordance with Exhibit B) or return to Controller in an encrypted format, at Controller's choice, all copies of Personal Data, including backup or archival copies, and (ii) promptly certify in writing to Controller when the measures described in subsection (i) hereof have been completed. Processor shall, and shall ensure that all Authorized Persons, comply with all Instructions provided by Controller with respect to the return or disposal of Personal Data. Any disposal of Personal Data must ensure that such data is rendered permanently unreadable and unrecoverable. Processor and/or Authorized Persons shall be excused from performing the foregoing obligations only if, and solely to the extent that, Applicable Law(s) explicitly prevent them from doing so.

3. Authorized Persons

3.1 Controller acknowledges and agrees that Processor may in the future (i) engage Authorized Persons, including Subprocessors to access and Process Personal Data in connection with the Services and (ii) from time to time engage additional third Parties for the purpose of providing the Services, including without limitation the Processing of Personal Data.

3.2 The Controller acknowledges and agrees that the Processor currently uses the Authorized Subprocessors to access and Process Personal Data as set forth on Exhibit C, and hereby consents to the use of such Authorized SubprocessorsProcessor may also retain any of its Affiliates to be subprocessors, and each Affiliate shall be deemed to be an Authorized Subprocessor.

3.3 If Processor intends to instruct additional sub-Processors in the future, Processor shall notify Controller thereof in writing (email to the email address(es) on record in Processor's account information for Controller is sufficient) and shall give Controller the opportunity to object to the engagement of the new sub-Processors within 30 days after being notified. The objection must be based on reasonable grounds (e.g. if Controller proves that significant Risks for the protection of its Personal Data exist at the sub-Processor). If Processor and Controller are unable to resolve such objection, either Party may terminate the Addendum by providing written notice to the other Party. Controller shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

3.4 If Controller does not object to the engagement of a third party in accordance with Section 4.2 after notice by Processor, such third party shall be deemed an Authorized Subprocessor for the purposes of this Addendum.

3.5 Processor shall ensure that all Authorized Subprocessors have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement by Processor, any Personal Data both during and after their engagement with Processor.

3.6 Processor shall, by way of contract or other legal act under European Union or European Union member state law or United Kingdom law (including without limitation approved codes of conduct and standard contractual clauses), ensure that every Authorized Subprocessor is subject to obligations regarding the Processing of Personal Data that are no less protective than those to which Processor is subject under this Addendum.

4.8. Processor shall be liable to Controller for the acts and omissions of Authorized Subprocessors to the same extent that Processor would itself be liable under this Addendum had it conducted such acts or omissions.

4. Incident, and Personal Data Breach Notification

4.1 Processor shall notify Controller without undue delay upon becoming aware of an Incident or a Personal Data Breach and shall, in a written report, provide such information that is within the Processor's knowledge to reasonably enable Controller to comply with its obligations under Applicable Laws with respect to such Incident or Personal Data Breach, including any obligation to report or notify such Incident or Personal Data Breach to Supervisory Authorities and/or Data Subjects, as applicable. Such report will include, to the extent that the Processor is aware of such information (i) a description of the nature of the Incident or Personal Data Breach, (ii) the categories and approximate number of Data Subjects and Personal Data sets affected or alleged to be affected, (iii) the likely consequences of the Incident or Personal Data Breach, and (iv) any measures that have been or may be taken to address and mitigate the Incident or Personal Data Breach.

4.2 As soon as reasonably practicable after providing the report described in Section 5.1, Processor shall provide Controller with a report on its initial findings regarding the Incident or Personal Data Breach, and thereafter shall provide regular updates describing subsequent findings with respect to such Incident or Personal Data Breach. As soon as reasonably practicable after Processor has concluded its examination of the Incident or Personal Data Breach, it shall provide Controller with a comprehensive final report regarding the Incident or Personal Data Breach.

4.3 To the extent a Data Breach of Incident is caused by the Processor and/or any relevant Authorized Subprocessor, the Processor and/or Authorized Subprocessor shall use all reasonable endeavors to attempt to mitigate and remedy any Incident or Personal Data Breach, and prevent any further Personal Data Breach or recurrence thereof, at Processor’s own expense and in accordance with Applicable Laws.

4.4 Neither Processor nor any Authorized Subprocessor shall publicly disclose any information regarding any Incident or Personal Data Breach without Controller’s prior written consent, *except that* Processor and any relevant Authorized Subprocessor may disclose any Suspected Incident, Incident or Personal Data Breach to (i) its own employees, customers, advisors, agents, or contractors, or (ii) where and to the extent explicitly compelled to do so by Applicable Laws, to applicable Supervisory Authorities and/or Data Subjects without Controller’s prior written consent.

4.5 Processor shall, and shall use reasonable efforts to ensure –that all relevant Authorized Subprocessor shall, at Processor’s expense, fully cooperate with Controller and provide reasonable assistance necessary for Controller to comply with any obligations under Applicable Laws with respect to an Incident or Personal Data Breach, including obligations to report or notify an Incident or Personal Data Breach to Supervisory Authorities and/or Data Subjects. Such assistance may include drafting disclosures, press releases and/or other communications for Controller with respect to such Incident or Personal Data Breach.

5. Data Subject Rights

5.1 Subject to Clauses 6.2 and 6.3, Processor shall, assist the Controller using the technical and organizational measures made available via the Processor's platform at the time. Such assistance shall be provided strictly to the extent necessary to support Controller’s response to requests by Data Subjects to exercise Data Subject Rights, including, specifically, a Data Subject’s right under Applicable Law to: (a) confirm whether his or her Personal Data has been or is being Processed; (b) access a copy of all Personal Data of his or hers that has been or is being Processed; (c) rectify or supplement his or her Personal Data; (d) transfer his or her Personal Data to another Controller; (e) confirm that his or her Personal Data has been or is being subject to Processing that constitutes automated decision-making; (f) restrict or cease the Processing of his or her Personal Data; and (g) withdraw consent to the Processing of his or her Personal Data held by Processor or any Authorized Person.

5.2 To the extent that the Controller does not have the ability to respond to a request from a Data Subject using such technical and organizational measures, the Processor shall, if requested by the Controller, make commercially reasonable efforts to assist the Controller in responding to such Data Subject Rights, provided that the Controller shall be responsible for any reasonable costs or expenses arising from Processor's provision of any such assistance, [which shall be payable within 30 days of the Processor's invoice].

5.3 The provision of assistance by Processor set out in Section 6.1 shall only apply only to the extent that the Processor is expressly required to provide such assistance under Applicable Law. Where Applicable Law does not require the Processor to provide any aspect of the assistance set out in Section 6.1, Processor shall not be obliged to provide such aspect of the assistance to Controller.

5.4 The Processor shall, without undue delay, notify Controller if Processor or an Authorized Subprocessor receives a request from a Data Subject to exercise a Data Subject Rights.) informing Controller in the event that Applicable Laws or any judicial, law enforcement, or Supervisory Authority operate to prevent Processor (or any Authorized Subprocessor) from performing the obligations described in this Section 6.1.

6. Transfers of Personal Data

6.1 Processor must obtain Controller's specific prior Instructions to perform International Data Transfers. Controller hereby authorizes Processor to perform International Data Transfers: (1) to any country subject to a valid adequacy decision of the EU Commission or UK Information Commissioner's Office; (2) to the extent authorized by Supervisory Authorities on the basis of an organization's binding corporate rules; or (3) on the basis of Standard Contractual Clauses in the form attached hereto as Exhibit A provided that they are duly executed between Processor and Controller. The Parties acknowledge and agree that if in future any Standard Contractual Clauses adopted by the European Commission or the UK Information Commissioner's Office are updated, amended, or replaced, then the Processor may notify the Controller of this in writing, and the Controller shall enter into such updated, amended or replaced Standard Contractual Clauses with the Processor, pursuant to such notification.

6.2 All authorizations of International Data Transfers in this Section 7 are expressly conditioned upon Processor's ongoing compliance with the requirements of Applicable Law applicable to International Data Transfers, and any applicable legal instrument for International Data Transfers. If such compliance is affected by circumstances outside of Processor's control, including circumstances affecting the validity of an applicable legal instrument, Controller and Processor will work together in good faith to reasonably resolve such non-compliance.

7. Actions and Access Requests

7.1 Upon Controller’s request, Processor shall make available to Controller all information available to Processor and to Authorized Subprocessors that Controller reasonably deems necessary to demonstrate compliance by Controller with its obligations under Applicable Laws (including in particular the GDPR, the UK GDPR or CCPA) relating to the Personal Data and the Processing conducted by Processor and Authorized Subprocessors.

7.2 Upon Controller’s request, Processor shall provide all necessary assistance to Controller in connection with any Data Protection Impact Assessment that Controller determines (in its discretion) it must conduct or cause to be conducted in order to comply with Applicable Laws, to the extent that such DPIA(s) relate to the Processing.

7.2.1 Upon Controller’s request, Controller shall provide all necessary assistance to Controller in connection with any consultation with a Supervisory Authority that Controller determines (in its discretion) it must undertake as a result of a DPIA, to the extent that such DPIA relates to the Processing.

7.3 Upon Controller’s request, Processor shall provide all necessary assistance to Controller in the event of any investigation, action, or request made by a Supervisory Authority, to the extent that such investigation, action, or request relates to the Personal Data or the Processing.

7.4 Upon Controller’s request, Processor shall provide Controller, and any Supervisory Authority with whom Controller is consulting or cooperating, with a designated contact for all queries and requests relating to the Processing of Personal Data.

7.5 In the event Processor determines that any Processing violates Applicable Laws (including the valid exercise of a Data Subject Right) or this Addendum, it shall immediately inform Controller and follow Instructions for stopping such Processing and/or remediating the violation.

7.6 Without limiting the foregoing, in the event of a change in Applicable Laws affecting this Addendum, Processor agrees to work in good faith with Controller to make any amendments to this Addendum pursuant to Section 13.2, and further agrees to make any changes to its Technical and Organizational Security Measures as are reasonably necessary to ensure continued compliance with Applicable Laws.

7.7 If so requested by Controller, Processor’s reasonable costs (including compensation for time) and expenses for providing any of the assistance set forth in this Section 8 shall be reimbursable by Controller, due and payable thirty (30) days from invoice.

8. Audit Rights

8.1 Processor shall maintain complete and accurate records in connection with Processor’s performance under this Addendum, and shall retain such records for a period of three (3) years after the termination or expiration of the Agreement.

9.2 Upon Controller written request and on at least 30 days’ notice, Processor will provide Controller with all information reasonably necessary to enable the Controller to conduct an audit to determine Processor’s compliance with this Addendum, to the extent that such information is within Processor control and Processor is not precluded from disclosing it by applicable law, a duty of confidentiality, or any other obligation owed to a third party.

9.3 In the event that Processor's records are not adequate to allow a determination of its performance, in the reasonable discretion of Controller, Controller may, upon written request and at least 30 days' notice to Processor, conduct an inspection of business operations solely to determine compliance with this Addendum and the Applicable Laws or have the same conducted by a qualified third party auditor bound by a duty of confidentiality subject to Processor approval, which shall not be unreasonably withheld. Controller shall bear any and all costs associated with the audit or inspection. Inspections at Processor premises must be carried out during regular business hours and without interrupting Processor business operations and cannot be conducted more frequently than once every 12 months. If Processor provides evidence of the agreed data protection obligations being correctly implemented, any inspections shall be limited to samples.

9. Limitation of Liability

9.1 The total liability of each of Controller and Processor (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the Agreement. Any exclusions of liability set out in the Agreement shall also apply in respect of this Addendum.

12. **California Consumer Privacy Act of 2018**

12.1. FloQast is a "Service Provider" as defined in CCPA Section 1798.140(v).

12.2. Customer discloses Personal Data to FloQast solely for: (i) a valid business purpose; and (ii) to permit FloQast to perform the Services.

12.3. FloQast is prohibited from: (i) selling Personal Data; (ii) retaining, using, or disclosing Personal Data for a commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing the Personal Data outside of the Addendum between FloQast and Processor.

12.4. FloQast understands the prohibitions outlined in Section 12.3.

13. Miscellaneous

13.1 This Addendum will terminate simultaneously and automatically with the termination of the Agreement, except that all provisions intending to survive shall survive, including specifically, Sections 1, 3.2, 4.5, 5, 8.3, 8.4, 9.1, 9.2, 10, 11 and 12.

13.2 This Addendum may be amended or modified only by a writing signed by both Parties. Processor acknowledges and agrees that the Controller (whether it is acting as a controller or a processor on behalf of another controller) may disclose this Addendum to third parties (including other controllers, data subjects and regulators) for purposes of demonstrating compliance with Applicable Laws.

13.3 This Addendum shall be governed by the law of the same jurisdiction as the Agreement, except where and to the extent that Applicable Laws require that the Addendum be governed by the law of another jurisdiction.

Exhibit A

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: [______]

Address: …[______]

Tel. …; fax …; e-mail: [______]

Other information needed to identify the organisation

…

(the data **exporter**)

And

Name of the data importing organisation: FloQast, Inc.

Address: 14721 Califa Street, Los Angeles, CA 91411

Tel. (818) 647-1168…; fax NA…; e-mail: legal@floqast.com…

Other information needed to identify the organisation:

…

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data

exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer [2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data

exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely …

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor’s obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at

least once a year. The list shall be available to the data exporter’s data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address: [______]

Other information necessary in order for the contract to be binding (if any):

	Signature …

On behalf of the data importer:

Name (written out in full): Erik Graham-Smith

Position: General Counsel

Address: 14721 Califa Street, Los Angeles, CA 91411

Other information necessary in order for the contract to be binding (if any):

	Signature …

Appendix 1

Details of Processing

Nature and Purpose of Processing: Processor will Process Personal Data on behalf of Controller for the purposes of providing the Services in accordance with the Agreement

Duration of Processing: : The term of the Agreement plus the period until Processor deletes all Personal Data processed on behalf of Controller in accordance with the Agreement

Categories of Data Subjects:

Individuals about whom Personal Data is provided to Processor via the Services by (or at the direction of) Controller or Controller’s end users, which may include without limitation Controller’s employees and contractors to whom Controller provides access to Processor’s Services.

Type of Personal Data: First Name, Last Name, Email, IP Address, Cookie Data, Geographic Location, Phone Number

Exhibit B

Security Measures

Processor will implement and maintain the security measures set out in this Exhibit B ("**Security Measures**"). Processor may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

Architecture, Data Segregation, and Data Processing

The Service is operated within the AWS Cloud and is designed to segregate and restrict customer data access based on business need. The Service's systems are designed upon the principle of least privilege where logical components reside in segregated AWS VPCs separated by stateful AWS security group firewalls and stateless Network ACLs. The Service architecture additionally provides effective logical data separation by use of cryptographic segmentation based on unique client specific encryption keys.

FloQast has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by FloQast and its sub-processors.

Security Controls

The Service includes a variety of configurable security controls that allow FloQast customers to tailor the security of the Service for their own use. The FloQast system provides several access control roles based on the organizational structure of each individual customer. All FloQast application security controls abide by OWASP and NIST standards. The Service integrates with several Single Sign on Providers, and where applicable recommends use of Single Sign On authentication in their configuration of the Service's security settings.

Information Security Management Program ("ISMP")

FloQast maintains a comprehensive information security management program that contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of FloQast's business; (b) the amount of resources available to FloQast; (c) the type of information that FloQast will store and process; and (d) the need for security and protection from unauthorized disclosure of such Customer Data. The ISMP is documented and updated based on changes in legal and regulatory requirements related to privacy and data security practices and industry standards applicable to the Service.

FloQast's ISMP is designed to:

- Protect the integrity, availability, and prevent the unauthorized disclosure by FloQast or its agents, of Customer Data in FloQast's possession or control;
- Protect against any anticipated threats or hazards to the integrity, and availability, and prevention of unauthorized disclosure of Customer Data by FloQast or its agents;
- Protect against unauthorized access, use, alteration, or destruction of Customer Data;
- Protect against accidental loss or destruction of, or damage to, Customer Data; and
- Safeguard information as set forth in any local, state or federal regulations by which FloQast may be regulated.

1. **Security Standards**. FloQast's ISMP includes adherence to and regular testing of the key controls, systems and procedures of its ISMP to validate that they are properly implemented and effective in addressing the threats and risks identified. Such testing includes:

a. Internal risk assessments;

b. External pen testing;

c. NIST guidance; and

d. SOC1 Type II (or successor standard) audits annually performed by accredited third-party auditors ("Audit Report") (FloQast will undergo its first SOC2 Type II audit in Quarter 1 of 2021, prior annual audits have been SOC1 Type 2).

2. **Security Audit Report**. FloQast provides its customers, upon their request, with a copy of FloQast's then-current Audit Report, including information as to whether the Security Audit revealed any material findings in the Service; and if so, the nature of each finding discovered.

3. **Assigned Security Responsibility**. FloQast assigns responsibility for the development, implementation, and maintenance of its Information Security Management Program, including:

a. Designating a security official with overall responsibility; and

b. Defining security roles and responsibilities for individuals with security responsibilities.

4. Relationship with Sub-processors. FloQast conducts reasonable due diligence and security assessments of sub-processors engaged by FloQast in the storing and/or processing of Customer Data ("Sub-processors"), and enters into agreements with Sub-processors that contain provisions similar or more stringent than those provided for in this security and privacy documentation.

5. Background Check. FloQast performs background checks on any employees who are to perform material aspects of the Service or have access to Customer Data.

6. Security Policy, Confidentiality. FloQast requires all personnel with access to Customer Data to acknowledge in writing, at the time of hire, that they will comply with the ISMP and protect all Customer Data at all times.

7. Security Awareness and Training. FloQast has mandatory security awareness and training programs for all FloQast personnel that address their implementation of and compliance with the ISMP.

8. Disciplinary Policy and Process. FloQast maintains a disciplinary policy and process in the event FloQast personnel violate the ISMP.

9. Access Controls. FloQast has in place policies, procedures, and logical controls that are designed:

a. To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;

b. To prevent personnel and others who should not have access from obtaining access; and

c. To remove access in a timely basis in the event of a change in job responsibilities or job status.

FloQast institutes:

a. Controls to ensure that only those FloQast personnel with an actual need-to-know will have access to any Customer Data;

b. Controls to ensure that all FloQast personnel who are granted access to any Customer Data are based on least-privilege principles;

c. Controls to require that user identifiers (User IDs) shall be unique and readily identify FloQast person to whom it is assigned, and no shared or group User IDs shall be used for FloQast personnel access to any Customer Data;

d. Password and other strong authentication controls that are made available to FloQast customers, so that customers can configure the Service to be in compliance with NIST guidance addressing locking out, uniqueness, reset, expiration, termination after a period of inactivity, password reuse limitations, length, expiration, and the number of invalid login requests before locking out a user; and

e. Periodic (no less than quarterly) access reviews to ensure that only those FloQast personnel with access to Customer Data still require it.

10. Physical and Environmental Security. FloQast maintains controls that provide reasonable assurance that access to physical servers at the production data center is limited to properly- authorized individuals and that environmental controls are established to detect, prevent, and control destruction due to environmental extremes. These controls include:

a. Logging and monitoring of unauthorized access attempts to the data center by the data center security personnel;

b. Camera surveillance systems at critical internal and external entry points to the data center;

c. Systems that monitor and control the air temperature and humidity at appropriate levels for the computing equipment; and

d. Uninterruptible Power Supply (UPS) modules and backup generators that provide back- up power in the event of an electrical failure.

11. Data Encryption.

a. Encryption of Transmitted Data: FloQast uses industry standard secure encryption methods to ensure all communications with the FloQast system is encrypted. All data is encrypted in transit using TLS 1.2 with ECDHE_RSA with P-256 as the key exchange and AES_128_GCM as the cipher.

b. Encryption of At-Rest Data: FloQast uses industry standard secure encryption methods designed to protect stored Customer Data at rest. All data at rest is stored encrypted by use of an application level unique client specific encryption key, which employs the authenticated AES-256-CBC cipher. Encryption keys are encrypted and protected at rest by use of the AWS KMS service. All data at rest is additionally stored in encrypted AWS EBS volumes which are further encrypted with the AWS KMS service.

c. Encryption of Backups: FloQast uses industry standard secure encryption methods designed to protect stored Customer Data at rest. All data at rest is stored encrypted by use of an application level unique client specific encryption key, which employs the authenticated AES-256-CBC cipher. Encryption keys are encrypted and protected at rest by use of the AWS KMS service. All data at rest is additionally stored in encrypted AWS EBS volumes which are further encrypted with the AWS KMS service.

12. **Disaster Recovery**. FloQast maintains policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

a. Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below

b. Disaster Recovery: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service, which includes requirements for the disaster plan to be tested on a regular basis, currently annually;

c. RPO / RTO: Recovery Point Objective is no more than 1 hour and Recovery Time Objective is no more than 24 hours;

d. Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources.

13. **Secure Development Practices**. FloQast adheres to the following development controls:

a. Development Policies: FloQast follows secure application development policies, procedures, and standards that are aligned to industry-standard practices; and

b. Training: FloQast provides employees responsible for secure application design, development, configuration, testing, and deployment appropriate (based on role) training by the security team regarding FloQast's secure application development practices.

14. **Malware Control**. FloQast employs industry-standard measures to test the Service to detect and remediate viruses, Trojan horses, worms, logic bombs, or other harmful code or programs designed to negatively impact the operation or performance of the Service.

15. **Data Integrity and Management**. FloQast maintains policies that ensure the following:

a. Segregation of Data: The Service includes logical controls, including encryption, to

segregate each customer's Customer Data from that of other customers; and

b. Back Up/Archival: FloQast performs full backups of the database(s) containing Customer Data no less than once per day and archival storage on no less than a weekly basis on secure server(s) or on other commercially acceptable secure media.

16. **Vulnerability Management**. FloQast maintains security measures to monitor the network and production systems, including error logs on servers, disks and security events for any potential problems. Such measures include:

a. Infrastructure Scans: FloQast performs regular vulnerability scans on all infrastructure components of its production and development environment. Vulnerabilities are remediated on a risk basis. FloQast installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

b. Application Scans: FloQast performs regular (as well as after making any major feature change or architectural modification to the Service) application vulnerability scans. Vulnerabilities are remediated on a risk basis. FloQast installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible;

c. External Application Vulnerability Assessment: FloQast engages third parties to perform network vulnerability assessments and penetration testing on an annual basis ("Vulnerability Assessment"). Reports from FloQast's then-current Vulnerability Assessment, together with any applicable remediation plans, will be made available to customers on written request.

Vulnerabilities are remediated on a risk basis. FloQast installs all medium, high, and critical security patches for all components in its production and development environment as soon as commercially possible.

17. **Change and Configuration Management**. FloQast maintains policies and procedures for managing changes to production systems, applications, and databases. Such policies and procedures include:

a. A process for documenting, testing and approving the promotion of changes into production;

b. A security patching process that requires patching systems in a timely manner based on a risk analysis; and

c. A process for FloQast to perform security assessments of changes into production.

18. **Secure Deletion**. FloQast maintains policies and procedures regarding the deletion of Customer Data in compliance with applicable NIST guidance and data protection laws, taking into account available technology so that Customer Data cannot be practicably read or reconstructed. Customer Data is deleted using secure deletion methods including digital shredding of encryption keys and hardware destruction in accordance with relevant guidelines.

19. **Intrusion Detection**. FloQast monitors the Service generally for unauthorized intrusions using traffic and activity-based monitoring systems. FloQast may analyze data collected by users' web browsers (e.g., device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plug-ins, enabled MIME types, etc.) for security purposes, including to detect compromised browsers, to help customers detect fraudulent authentications, and to ensure that the Service functions properly.

20. **Incident Management**. FloQast has in place a security incident response plan that includes procedures to be followed in the event of any unauthorized disclosure of Customer Data by FloQast or its agents of which FloQast becomes aware to the extent permitted by law (such unauthorized disclosure defined herein as a "Security Breach"). The procedures in FloQast's security incident response plan include:

a. Roles and responsibilities: formation of an internal incident response team with a response leader;

b. Investigation: assessing the risk the incident poses and determining who may be affected;

c. Communication: internal reporting as well as a notification process in the event of a Security Breach;

d. Recordkeeping: keeping a record of what was done and by whom to help in subsequent analyses; and

e. Audit: conducting and documenting a root cause analysis and remediation plan.

FloQast typically notifies customers of significant system incidents by email to the listed admin contact, and for availability incidents lasting more than one hour, may invite impacted customers to join a conference call about the incident and FloQast's response.

21. **Security Breach Management**.

a. Notification: In the event of a Security Breach, FloQast notifies impacted customers of such Security Breach. FloQast cooperates with an impacted customer's reasonable request for information regarding such Security Breach, and FloQast provides regular updates on any such Security Breach and the investigative action and corrective action(s) taken.

b. Remediation: In the event of a Security Breach, FloQast, at its own expense, (i) investigates the actual or suspected Security Breach, (ii) provides any affected customer with a remediation plan, to address the Security Breach and to mitigate the incident and reasonably prevent any further incidents, (iii) remediates the effects of the Security Breach in accordance with such remediation plan, and (iv) reasonably cooperates with any affected customer and any law enforcement or regulatory official investigating such Security Breach.

22. **Logs**. FloQast provides procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports. FloQast (i) backs-up logs on a daily basis, (ii) implements commercially reasonable measures to protect such logs from unauthorized modification or erasure, and (iii) retains such logs in compliance with FloQast's data retention policy. If there is suspicion of inappropriate access to the Service, FloQast has the ability to provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis.

Exhibit C

Authorized Subprocessors

AWS American West Region (OR and CA, USA);

Pendo.io (Raleigh, NC USA);

MongoDB (NY, NY, USA);

Coalfire Labs (Westminster, CO, USA);

Deloitte (NY, NY, USA)