flooid

Data Processing Addendum

This Data Processing Addendum ("Data Processing Addendum") is incorporated into and forms part of the Subscription Agreement ("Agreement") between Flooid and Customer. Generally, Flooid acknowledges that Customer is the Data Controller in relation to the processing of Personal Information and Customer appoints Flooid as the Data Processor of such Personal Information. In the event of a conflict between this Data Processing Addendum and the Agreement, unless otherwise expressly provided, the Agreement will control. All capitalized terms not defined herein have the meaning ascribed to them in the Agreement.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an addendum to Subscription Agreement.

(A) Definitions

"Agent" shall mean the employees, subcontractors of the respective parties.

"CCPA" shall mean the California Consumer Privacy Act, Cal. Civ Code § 1798.100 et seq. and its implementing regulations.

"Data Breach" shall mean any unauthorized disclosure, access, use, loss, damage or destruction of any Personal Information (as defined below) provided by either party to the other.

"Data Controller" shall mean (i) the party that provided the Personal Information for Processing; or (ii) Data Controller as defined in the Data Protection & Privacy Laws.

"Data Processor" shall mean the party that (i) processes the Personal Information on behalf of the Data Controller, or (ii) carries out any operation or set of operations on Personal Information or on sets of Personal Information on behalf of the Data Controller, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; or (iii) Data Processor as defined in the Data Protection & Privacy Laws.

"Data Protection & Privacy Laws" means all data protection and privacy laws, including local, state, (e.g., CCPA), national and/or foreign laws, treaties, and/or regulations, the GDPR and UK GDPR (as each are defined below), to the extent applicable to each respective party in its roll in Processing Personal Information.

"GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679).

"Malware" shall mean back doors, traps, disabling routines, worms, viruses, spyware, ransomware, or other malicious or damaging code.

"Personal Information" shall mean any data

a) that can be reasonably linked to a living individual with or without correlation to other information that either party could reasonably be expected to access, and is not solely information that is

in the public domain or routinely provided by either party to the other party to facilitate business communication in support of the Agreement, or

b) relating to an identified or identifiable natural person, an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; or

c) defined as Personal Information in the Data Protection & Privacy Laws

"Processing" shall mean (i) any operation or set of operations which is performed on Personal Information or on sets of Personal Information, 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; or (ii) Processing as defined in the Data Protection & Privacy Laws.

"Security Incident" shall mean any event that negatively affects the confidentiality (e.g., Data Breach), integrity (e.g., data corruption), or availability (e.g., denial of service) of Systems (as defined below) or the services relevant to this Agreement. "Systems" shall mean networks, systems, applications, services, and data that together deliver a business function.

"Sensitive Information" shall mean the subset of Personal Information that

a) directly or indirectly contains or can be linked with financial, medical, religious, or political data, or

b) is defined as Sensitive Information in the Data Protection & Privacy Laws.

"UK GDPR" has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

(B) Processing

a) Both parties agree that when acting as a Data Controller with respect to the other party, a Data Controller:

i. shall limit the volume and sensitivity of Personal Information exchanged to the minimum necessary and sufficient to complete the agreed Processing;

ii. shall agree with the Data Processor as to the minimum and sufficient security controls in writing before transferring Personal Information for Processing;

iii. agrees that a Data Processor may reasonably act on the assumption that data is not Personal Information unless otherwise agreed between the parties in writing; and

iv. shall not provide the Data Processor with Sensitive Information.

b) Both parties agree that when acting as Data Processor with respect to the other party, a Data Processor:

i. shall only process Personal Information for the specific purpose that the Personal Information was provided by the Data Controller;

ii. shall implement appropriate technical and organizational measures as agreed with the Data Controller and shall comply with relevant Data Protection & Privacy Laws; and

iii. shall only retain the Personal Information as mutually agreed or required for processing hereunder, including but not limited to legal or regulatory requirements, and shall return the Personal Information to the other party upon termination or expiration of the Agreement.

c) Neither Party will engage a third-party Processor for the Personal Information without prior written authorization from the Data Controller.

(C) Audit

a) Either party may assess or audit the other party's Information Security Program (as defined below) to determine compliance with this Data Processing Addendum.

b) The scope of the assessments or audits is limited to Systems in which Personal Data of the Data Controller is held, stored, processed or transmitted, and the systems and processes that manage the security of the processing system.

c) Such assessments or audits may be conducted no more frequently than annually or when significant change has occurred by each party or party's Agents subject to agreement between the parties as to the date and time of such audit.

d) For the avoidance of doubt, audits will only be carried out during Business Hours.

e) Parties agree to make available to each other such reasonably requested resources (e.g., personnel and documentation) required for completion of audit activities provided that the auditing party makes payment for the other party's costs on a time and material basis in complying with this clause C (costs to be agreed upon between the parties prior to being incurred).

f) Parties agree to develop and provide an action plan for remediation of any significant security weaknesses identified in the Systems, with remediation to occur in a reasonable timeframe commensurate with the significance of the security weaknesses. If the parties, acting reasonably, are unable to agree on an appropriate remediation plan and timeline within a reasonable period of time, then the dispute resolution process may be initiated.

(D) Obligations

a) In addition to other obligations under this Data Processing Addendum, the parties' have the following obligations:

i. each party shall be solely responsible for its Agents. Any breach of this Data Processing Addendum by a party's Agents constitutes a breach of this Data Processing Addendum by that party.

ii. each party shall develop, implement and continue to maintain a written, comprehensive information security program ("Information Security Program") and implement and continues to maintain

commercially reasonable security controls commensurate with the sensitivity of Personal Information and Confidential Information exchanged between the parties.

iii. each party shall comply with all applicable federal, state and local data security or privacy laws, ordinances, regulations and other requirements of public authorities where such laws relate to the delivery of the services.

iv. each party acting as Data Controller shall inform the other party as Data Processor of federal, state and local data security or privacy, ordinances, regulations with which the Data Processor is required to comply. The Data Controller shall provide all reasonable assistance to the Data Processor to understand and comply with such regulations, including assistance with data subject access requests.

v. the Customer shall process all Customer Personal Information in compliance with the Data Protection & Privacy Laws.

(E) Data Breach

a) In the event of any Data Breach or other Security Incident by one party that impacts the other party, the acting party shall:

i. as soon as reasonably practicable notify the other party of any facts known to them regarding the Data Breach or other Security Incident.

ii. provide a summary of the cause of the Data Breach or Security Incident, to the extent permissible by law and without breaching any other contracts.

iii. develop and provide an action plan for remediation of any significant security weaknesses identified in the Systems, with remediation to occur in a reasonable timeframe commensurate with the significance of the security weaknesses. If the parties, acting reasonably, are unable to agree on an appropriate remediation plan and timeline within a reasonable period of time, then the parties agree to mediate the remediation plan and timeline with a mediator mutually agreed upon by the parties. The cost of mediation shall be split equally between the parties.

(F) Access to Systems

a) In the event that a party provides access to the other to one or more Systems, the other party agrees

i. that Systems are owned by the party providing the access.

ii. that the party providing access reserves the right to monitor use of Systems.

iii. that the other party should have no expectation of privacy with regard to use of Systems.

iv. that all information stored, processed, transmitted or accessed will be considered Confidential Information.

v. that any data supplied may be stored, processed, and transmitted at the sole determination of the party providing access.

b) Each party agrees

i. that it will not use Systems except as expressly authorized by the other party.

ii. to maintain strict control of all usernames, passwords, and access lists to Systems.

iii. to ensure access credentials are available to only authorized Agents, as necessary to perform or utilize services under this Data Processing Addendum.

iv. to immediately remove or coordinate the removal of such access for persons no longer authorized to use Systems.

v. to inform the other party immediately if there is reason to believe unauthorized access may exist.

vi. to cause its Agents who gain access to Systems to maintain the confidential nature of all Confidential Information.

vii. to not attempt to introduce Malware or otherwise attempt to alter, destroy or damage the Systems.