# FluidStack - Data Protection Addendum

This Data Protection Addendum was published on 29th November 2021.

## 1. Introduction

1.1 This Data Protection Addendum (as updated from time to time) is incorporated into FluidStack's Terms of Service and Terms of Supply (available at https://www.fluidstack.io/).

1.2 Defined terms in this Data Protection Addendum shall have the meaning given in the Terms of Service and Terms of Supply and the same rules of interpretation apply.

1.3 In addition, in this Data Protection Addendum the following definitions have the meanings given below:

| | |
|---|---|
| **'Applicable Law'** | *applicable laws of the European Union (EU), the European Economic Area (EEA) or any of the EU or EEA's member states from time to time together with applicable laws in the United Kingdom from time to time;* |
| **'Appropriate Safeguards'** | such legally enforceable mechanism(s) for transfers of Personal Data as may be permitted under Data Protection Laws from time to time; |
| **'Business Contact Information'** | the names, mailing addresses, email addresses, and phone numbers regarding the other party's employees or consultants including such information regarding the other party's suppliers and customers, used as part of maintaining its business relationships. |
| **'Controller'** | has the meaning given to that term in Data Protection Laws; |
| **'Data Controller'** | has the meaning given to it in clause 2.2; |
| **'Data Processor'** | has the meaning given to it in clause 2.2; |
| **'Data Protection Laws'** | as applicable and binding on the Controller or Processor and/or the Cloud Services:<br>(a) in the United Kingdom:<br>(i) the Data Protection Act 2018; and<br>(ii) the GDPR, and/or any corresponding or equivalent national laws or regulations;<br>(b) in member states of the European Union (**'EU'**) and/or European Economic Area (**'EEA'**): the GDPR and all relevant EU and EEA member state laws or regulations giving effect to or corresponding with any of the GDPR; and<br>(c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time; |
| **'Data Protection Losses'** | all liabilities, including all:<br>(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, |

| | |
|---|---|
| | losses and damages (including relating to material or non-material damage); and<br>(b) to the extent permitted by Applicable Law:<br>(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;<br>(ii) compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and<br>(iii) the reasonable costs of compliance with investigations by a Supervisory Authority; |
| **'Data Subject'** | has the meaning given to that term in Data Protection Laws; |
| **'Data Subject Request'** | a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws; |
| **'GDPR'** | the General Data Protection Regulation, Regulation (EU) 2016/679; |
| **'International Organisation'** | an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries; |
| **'International Recipient'** | (a) any countries outside the United Kingdom and/or the European Economic Area; or<br>(b) any International Organisation(s); |
| **'List of Sub-Processors'** | the latest version of the list of Sub-Processors used by Data Processor, as updated and notified to Data Controller by Data Processor from time-to-time, including on its website; |
| **'Personal Data'** | has the meaning given to that term in Data Protection Laws; |
| **'Personal Data Breach'** | any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data; |
| **'processing'** | has the meanings given to that term in Data Protection Laws (and related terms such as 'process' have corresponding meanings); |
| **'Processing Instructions'** | has the meaning given to that term in paragraph 4.1(a); |
| **'Processor'** | has the meaning given to that term in Data Protection Laws; |
| **'Protected Data'** | Personal Data in the Customer Data; |
| **'Sub-Processor'** | another Processor engaged by Data Processor for carrying out processing activities in respect of the Protected Data on behalf of Data Controller; and |
| **'Supervisory Authority'** | any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws. |

2. **Processor and Controller**

2.1 The parties agree that:

(a) for the Protected Data, the Customer shall be the Controller and the Third-Party Provider shall be the Processor. Nothing in this Agreement relieves the Customer of any responsibilities or liabilities under any Data Protection Laws; and

(b) to the extent that Customer or Third-Party Provider provides Business Contact Information to FluidStack, Customer or Third-Party Provider (as applicable) shall be the Controller and FluidStack shall be the Processor of that Business Contact Information. FluidStack may use that Business Contact Information for contract management, payment processing, service offering, and business development purposes related to the Agreement and such other purposes as set out in FluidStack's Privacy Notice (available at https://www.fluidstack.io/).

2.2 In this Data Protection Addendum, where FluidStack, Customer or Third-Party Provider is acting in its capacity as a:

(a) Controller, the obligations and responsibilities of Data Controller shall apply to that party (as relevant); or

(b) Processor, the obligations and responsibilities of Data Processor shall apply to the party (as relevant).

2.3 To the extent the Customer is not sole Controller of any Protected Data it warrants that it has full authority and authorisation of all relevant Controllers to instruct the Data Processor to process the Protected Data in accordance with the Agreement.

2.4 The Data Processor shall process Protected Data in compliance with:

(a) the obligations of Processors under Data Protection Laws in respect of the performance of its and their obligations under the Agreement; and

(b) the terms of the Agreement.

3. **Instructions and details of processing**

3.1 Insofar as Data Processor processes Protected Data on behalf of Data Controller, Data Processor:

(a) unless required to do otherwise by Applicable Law, shall (and shall take steps to ensure each person acting under its authority shall) process the Protected Data only on and in accordance with Data Controller's documented instructions as set out in this paragraph 4.1 and paragraphs 4.2 and 4.3 (including when making a transfer of Protected Data to any International Recipient), as updated from time to time (**'Processing Instructions'**);

(b) if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify Data Controller of any such requirement before processing the Protected Data (unless Applicable Law prohibits such information on important grounds of public interest); and

(c) shall promptly inform Data Controller if Data Processor becomes aware of a Processing Instruction that, in Data Processor's opinion, infringes Data Protection Laws, provided that to the maximum extent permitted by mandatory law, Data Processor shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing in accordance with Data Controller's Processing Instructions following Data Controller's receipt of that information.

3.2 Data Controller acknowledges and agrees that the execution of any computer command to process (including deletion of) any Protected Data made in the use of any of the Cloud Services by a customer of Customer will be a Processing Instruction (other than to the extent such command is not fulfilled due to technical, operational or other reasons). Data Controller shall ensure that customers of Customer do not execute any such command unless authorised by Data Controller (and by all other relevant Controller(s)) and acknowledge that if any Protected Data is deleted pursuant to any such command Data Processor is under no obligation to seek to restore it.

3.3 Subject to where the contrary appears in the Agreement, the processing of the Protected Data by Data Processor under the Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in Appendix 1.

## 4. Technical and organisational measures

4.1 Taking into account the nature of the processing, Data Processor shall implement and maintain, at its cost and expense, the technical and organisational measures:

(a) in relation to the processing of Protected Data by Data Processor; and

(b) to assist Data Controller insofar as is possible in the fulfilment of Data Controller's obligations to respond to Data Subject Requests relating to Protected Data, in each case at Data Controller's cost on a time and materials basis in accordance with Data Processor's standard pricing terms, as notified to Data Controller by Data Processor from time-to-time.

## 5. Using staff and other processors

5.1 Data Processor shall not engage any Sub-Processor for carrying out any processing activities in respect of the Protected Data except in accordance with the Agreement without Data Controller's written authorisation of that specific Sub-Processor (such authorisation not to be unreasonably withheld, conditioned or delayed).

5.2 Data Controller authorises the appointment of each of the Sub-Processors identified on the List of Sub-Processors as updated from time to time.

5.3 Data Processor shall:

(a) prior to the relevant Sub-Processor carrying out any processing activities in respect of the Protected Data, appoint each Sub-Processor under a written contract containing materially the same obligations as under paragraphs 2 to 14 (inclusive) that is enforceable by Data Processor (including those relating to sufficient guarantees to implement appropriate technical and organisational measures);

(b) ensure each such Sub-Processor complies with all such obligations; and

(c) remain fully liable for all the acts and omissions of each Sub-Processor as if they were its own.

5.4 Data Processor shall ensure that all persons authorised by it (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation to keep the

Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case Data Processor shall, where practicable and not prohibited by Applicable Law, notify Data Controller of any such requirement before such disclosure).

## 6. Assistance with compliance and Data Subject rights

6.1 Data Processor shall refer all Data Subject Requests it receives to Data Controller without undue delay. Data Controller shall pay Data Processor for all work, time, costs and expenses incurred in connection with such activity, calculated on a time and materials basis at the Data Processor's standard pricing terms, as notified to Data Controller by Data Processor from time-to-time.

6.2 Data Processor shall provide such reasonable assistance as Data Controller reasonably requires (taking into account the nature of processing and the information available to Data Processor) to Data Controller in ensuring compliance with Data Controller's obligations under Data Protection Laws with respect to:

(a) security of processing;

(b) data protection impact assessments (as such term is defined in Data Protection Laws);

(c) prior consultation with a Supervisory Authority regarding high risk processing; and

(d) notifications to the Supervisory Authority and/or communications to Data Subjects by Data Controller in response to any Personal Data Breach,

provided Data Controller shall pay Data Processor for all work, time, costs and expenses incurred in connection with providing the assistance in this paragraph 7.2, calculated on a time and materials basis at the Data Processor's standard pricing terms, as notified to Data Controller by Data Processor from time-to-time.

## 7. International data transfers

7.1 Subject to paragraph 8.2, Data Processor shall not transfer, or otherwise directly or indirectly disclose, any Protected Data to any International Recipient without the prior written consent of Data Controller except where Data Processor is required to transfer the Protected Data by Applicable Law (and shall inform Data Controller of that legal requirement before the transfer, unless those laws prevent it doing so).

7.2 Data Controller agrees that Data Processor may transfer any Protected Data for *the purposes referred to in paragraph* 4.3 to any International Recipient, provided all transfers by Data Processor of Protected Data to an International Recipient (and any onward transfer) shall (to the extent required under Data Protection Laws) be effected by way of Appropriate Safeguards and in accordance with Data Protection Laws. The provisions of the Agreement shall constitute Data Controller's instructions with respect to transfers in accordance with paragraph 4.1(a).

7.3 Data Controller acknowledges that due to the nature of cloud services, the Protected Data may also be transferred to other geographical locations in connection with use of the Cloud Services further to access and/or computerised instructions initiated by customers of Customer. Data Controller acknowledges that Data Processor does not control such processing and Data Controller shall ensure that customers of Customer (and all others acting on its behalf) only initiate the transfer of Protected Data to other geographical locations if Appropriate Safeguards are in place and that such transfer is in compliance with all Applicable Laws.

8. **Information and audit**

8.1 Data Processor shall maintain, in accordance with Data Protection Laws binding on Data Processor, written records of all categories of processing activities carried out on behalf of Data Controller.

8.2 Data Controller may by written notice to Data Processor request information regarding Data Processor's compliance with the obligations placed on it under this Data Protection Addendum. On receipt of such request Data Processor shall provide Data Controller (or auditors mandated Data Controller) with a copy of the latest third-party certifications and audits to the extent made generally available to its customers. Such copies are confidential to Data Processor and shall be Data Processor' Confidential Information for the purposes of the Agreement.

8.3 Data Processor shall, on request by Data Controller, in accordance with Data Protection Laws, make available to Data Controller such information as is reasonably necessary to demonstrate Data Processor's compliance with its obligations under this Data Protection Addendum and Article 28 of the GDPR (and under any Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by Data Controller (or another auditor mandated by Data Controller) for this purpose provided:

(a) such audit, inspection or information request is reasonable, limited to information in Data Processor's (or any Sub-Processor's) possession or control and is subject to Data Controller giving Data Processor reasonable prior notice of such audit, inspection or information request;

(b) the parties (each acting reasonably and consent not to be unreasonably withheld or delayed) shall agree the timing, scope and duration of the audit, inspection or information release together with any specific policies or other steps with which Data Controller or third party auditor shall comply (including to protect the security and confidentiality of other customers, to ensure Data Processor is not placed in breach of any other arrangement with any other customer and so as to comply with the remainder of this paragraph 9.3);

(c) all costs of such audit or inspection or responding to such information request shall be borne by Data Controller, and Data Processor's costs, expenses, work and time incurred in connection with such audit or inspection shall be reimbursed by Data Controller on a time and materials basis in accordance with Data Processor's standard pricing terms, as notified to Data Controller by Data Processor from time to time;

(d) Data Controller's rights under this paragraph 9.3 may only be exercised once in any consecutive *12*-month period, unless otherwise required by a Supervisory Authority or if Data Controller (acting reasonably) believes Data Processor is in breach of this Data Protection Addendum;

(e) Data Controller shall promptly (and in any event within three Business Days) report any non-compliance identified by the audit, inspection or release of information to Data Processor;

(f) Data Controller shall ensure that all information obtained or generated by Data Controller or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure required by Applicable Law);

(g) Data Controller shall ensure that any such audit or inspection is undertaken during normal business hours, with minimal disruption to the businesses of Data Processor and each Sub-Processor; and

(h) Data Controller shall ensure that each person acting on its behalf in connection with such audit or inspection (including the personnel of any third party auditor) shall not by any act or omission cause or contribute to any damage, destruction, loss or corruption of or to any systems, equipment or data in the control or possession of Data Processor or any Sub-Processor whilst conducting any such audit or inspection.

## 9. Breach notification

9.1 In respect of any Personal Data Breach involving Protected Data, Data Processor shall, without undue delay:

(a) notify Data Controller of the Personal Data Breach; and

(b) provide Data Controller with details of the Personal Data Breach.

## 10. Deletion of Protected Data and copies

Following the end of the provision of the Cloud Services (or part) (as applicable) relating to the processing of Protected Data, Data Processor shall dispose of Protected Data in accordance with its obligations under the Agreement. Data Processor shall have no liability (howsoever arising, including in negligence) for any deletion or destruction of any such Protected Data undertaken in accordance with the Agreement.

## 11. Compensation and claims

11.1 Subject to the Terms of Service, Data Processor shall be liable for Data Protection Losses (howsoever arising, whether in contract, tort (including negligence) or otherwise) under or in connection with the Agreement:

(a) only to the extent caused by the processing of Protected Data under the Agreement and directly resulting from Data Processor's breach of the Agreement; and

(b) in no circumstances to the extent that any Data Protection Losses (or the circumstances giving rise to them) are contributed to or caused by any breach of the Agreement by Data Controller (including in accordance with paragraph 4.1(c)).

11.2 If a party receives a compensation claim from a person relating to processing of Protected Data in connection with the Agreement or the Cloud Services, it shall promptly provide the other party with notice and full details of such claim. The party with conduct of the action shall:

(a) make no admission of liability nor agree to any settlement or compromise of the relevant claim without the prior written consent of the other party (which shall not be unreasonably withheld or delayed); and

(b) consult fully with the other party in relation to any such action but the terms of any settlement or compromise of the claim will be exclusively the decision of the party that is responsible under the Agreement for paying the compensation.

11.3 The parties agree that Data Controller shall not be entitled to claim back from Data Processor any part of any compensation paid by Data Controller in respect of such damage to the extent that

Data Controller is liable to indemnify or otherwise compensate Data Processor in accordance with the Agreement.

11.4 This paragraph 12 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

(a) to the extent not permitted by Applicable Law (including Data Protection Laws); and

(b) that it does not affect the liability of either party to any Data Subject.

## 12. Data Controller obligations

12.1 Data Controller shall ensure that it, its Affiliates and, where applicable, its customers shall at all times comply with:

(a) all Data Protection Laws in connection with the processing of Protected Data, the use of the Cloud Services (and each part) and the exercise and performance of its respective rights and obligations under the Agreement, including maintaining all relevant regulatory registrations and notifications as required under Data Protection Laws; and

(b) the terms of the Agreement.

12.2 Data Controller warrants, represents and undertakes, that at all times:

(a) all Protected Data (if processed in accordance with the Agreement) shall comply in all respects, including in terms of its collection, storage and processing, with Data Protection Laws;

(b) the Protected Data is accurate and up to date;

(c) it shall establish and maintain adequate security measures to safeguard Protected Data in its possession or control from unauthorised access and copying and maintain complete and accurate backups of all Protected Data provided to Data Processor (or anyone acting on its behalf) so as to be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption of such Protected Data by Data Processor or any other person; and

(d) all instructions given by it to Data Processor in respect of Personal Data shall at all times be in accordance with Data Protection Laws.

## 13. Survival

This Data Protection Addendum (as updated from time to time) shall survive termination (for any reason) or expiry of the Agreement and continue until no Protected Data remains in the possession or control of Data Processor or any Sub-Processor, except that paragraphs 11 to 14 (inclusive) shall continue indefinitely.

Appendix 1

## Data processing details

**Subject-matter of processing:**

- Performance of respective rights and obligations under the Agreement and delivery and receipt of the Cloud Services under the Agreement.

**Duration of the processing:**

- Until the earlier of final termination or final expiry of the Agreement, except as otherwise expressly stated in the Agreement.

**Nature and purpose of the processing:**

- processing in accordance with the rights and obligations of the parties under the Agreement;
- processing as reasonably required to provide the Cloud Services; and/or
- processing as initiated, requested or instructed by Customer in a manner consistent with the Agreement.

**Type of Personal Data:**

Includes any types of Protected Data uploaded to the cloud infrastructure.

**Categories of Data Subjects:**

- Includes any Data Subject about whom Protected Data is uploaded to the cloud infrastructure.

**Special categories of Personal Data**:

- Not applicable