crunchy data

Data Processing Addendum

THIS DATA PROCESSING ADDENDUM is entered into as of the Addendum Effective Date by and between: (1) **CRUNCHY DATA SOLUTIONS, INC.**, a company incorporated and registered in the State of Delaware whose registered office is at 162 Seven Farms Drive, Suite 220, Charleston, SC 29492 ("**Crunchy Data**"); and (2) the natural or legal person that is a party to the Agreement with Crunchy Data ("**Customer**").

1. INTERPRETATION

1.1. In this Data Processing Addendum the following terms shall have the meanings set out in this Paragraph 1, unless expressly stated otherwise:

(a) "**Addendum Effective Date**" means the effective date of the Agreement.

(b) "**Agreement**" means the Crunchy Bridge Terms of Service at https://www.crunchybridge.com/terms.

(c) "**Cessation Date**" has the meaning given in Paragraph 9.1.

(d) "**Customer Personal Data**" means any Personal Data Processed by or on behalf of Crunchy Data on behalf of Customer under the Agreement.

(e) "**Data Subject Request**" means the exercise by Data Subjects of their rights under, and in accordance with, Chapter III of the GDPR, in respect of Customer Personal Data.

(f) "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

(g) "**Delete**" means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed, and "**Deletion**" shall be construed accordingly.

(h) "**EEA**" means the European Economic Area.

(i) "**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

(j) "**GDPR**" means the UK GDPR and/or EU GDPR (as applicable), together with any applicable implementing or supplementary legislation in any member state of the EEA or the UK (including the UK Data Protection Act 2018). References to "**Articles**" and "**Chapters**" of, and other relevant defined terms in, the GDPR shall be construed accordingly.

(k) "**Personnel**" means a person's employees, agents, consultants or contractors.

(l) "**Post-cessation Storage Period**" has the meaning given in Paragraph 9.2.

(m) "**Relevant Body**":

(i) in the context of the UK and the UK GDPR, means the UK Information Commissioner's Office and/or UK Government (as and where applicable); and/or

(ii) in the context of the EEA and EU GDPR, means the European Commission.

(n) “**Restricted Country**”:

(i) in the context of the UK, means a country or territory outside the UK; and

(ii) in the context of the EEA, means a country or territory outside the EEA (which shall, as and where applicable, be interpreted in line with Article FINPROV.10A(1) of the Trade and Cooperation Agreement between the EU and the UK),

that the Relevant Body has not deemed to provide an ‘adequate’ level of protection for Personal Data pursuant to a decision made in accordance Article 45(1) of the GDPR.

(o) “**Restricted Transfer**” means the disclosure, grant of access or other transfer of Personal Data to any person, which would be prohibited without a legal basis therefor under Chapter V of the GDPR.

(p) “**Services**” means those services and activities to be supplied to or carried out by or on behalf of Crunchy Data for Customer pursuant to the Agreement.

(q) “**Standard Contractual Clauses**” means the standard contractual clauses issued or approved by the Relevant Body (from time-to-time) for the transfer of Personal Data from Controllers to Processors established in Restricted Countries, the current form of which is attached hereto as Annex 2.

(r) “**Subprocessor**” means any third party appointed by or on behalf of Crunchy Data to Process Customer Personal Data.

(s) “**Supervisory Authority**”:

(i) in the context of the UK and the UK GDPR, means the UK Information Commissioner’s Office; and

(ii) in the context of the EEA and EU GDPR, shall have the meaning given to that term in Article 4(21) of the EU GDPR.

(t) “**UK GDPR**” means the EU GDPR as it forms part of UK law by virtue of section 3 of the European Union (Withdrawal) Act 2018, as amended (including by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019).

1.2. In this Data Processing Addendum:

(a) the terms, “**Controller**”, “**Processor**”, “**Personal Data**”, “**Personal Data Breach**” and “**Process/Processing/Processed**” shall have the meaning ascribed to the corresponding terms in the GDPR; and

(b) unless otherwise defined in this Data Processing Addendum, all capitalised terms in this Data Processing Addendum shall have the meaning given to them in the Agreement.

1.3. Customer warrants and represents that the Processing delegated to Crunchy Data under the Agreement is subject to the territorial scope of the GDPR as determined in accordance therewith (including pursuant to Article 3 of the GDPR). Customer further agrees that to the extent that the same is not in fact subject to the territorial scope of the GDPR, this Data Processing Addendum shall be deemed automatically void with effect from the Addendum Effective Date without requirement of notice.

2. PROCESSING OF CUSTOMER PERSONAL DATA

2.1. The Parties acknowledge that:

(a) Crunchy Data acts as a Processor; and

(b) Customer acts as the Controller.

2.2. Crunchy Data shall:

(a) comply with the GDPR in Processing Customer Personal Data; and

(b) not Process Customer Personal Data other than:

(i) on Customer's instructions (subject always to Paragraph 2.9); and

(ii) as required by applicable laws.

2.3. To the extent permitted by applicable laws, Crunchy Data shall inform Customer of:

(a) any Processing to be carried out under Paragraph 2.2(b)(ii); and

(b) the relevant legal requirements that require it to carry out such Processing,

before the relevant Processing of that Customer Personal Data.

2.4. Customer instructs Crunchy Data to Process Customer Personal Data as necessary:

(a) to provide the Services to Customer; and

(b) to perform Crunchy Data's obligations and exercise Crunchy Data's rights under the Agreement.

2.5. Annex 1 (*Data Processing Details*) sets out certain information regarding Crunchy Data's Processing of Customer Personal Data as required by Article 28(3) of the GDPR.

2.6. Customer may amend Annex 1 (*Data Processing Details*) on written notice to Crunchy Data from time to time as Customer reasonably considers necessary to meet any applicable requirements of the GDPR.

2.7. Nothing in Annex 1 (*Data Processing Details*) (including as amended pursuant to Paragraph 2.6) confers any right or imposes any obligation on any party to this Data Processing Addendum.

2.8. Where Crunchy Data receives an instruction from Customer that, in its reasonable opinion, infringes the GDPR, Crunchy Data shall inform Customer.

2.9. Customer acknowledges and agrees that any instructions issued by Customer with regards to the Processing of Customer Personal Data by or on behalf of Crunchy Data pursuant to or in connection with the Agreement:

(a) shall be strictly required for the sole purpose of ensuring compliance with the GDPR; and

(b) shall not relate to the scope of, or otherwise materially change, the Services to be provided by Crunchy Data under the Agreement.

2.10. Notwithstanding anything to the contrary herein, Crunchy Data may terminate the Agreement in its entirety upon written notice to Customer with immediate effect if Crunchy Data considers (in its reasonable discretion) that:

(a) it is unable to adhere to, perform or implement any instructions issued by Customer due to the technical limitations of its systems, equipment and/or facilities; and/or

(b) to adhere to, perform or implement any such instructions would require disproportionate effort (whether in terms of time, cost, available technology, manpower or otherwise).

2.11. Customer represents and warrants on an ongoing basis that, for the purposes of Article 6 of the GDPR, and (where applicable) Article 9 and/or Article 10 of the GDPR, there is, and will be throughout the term of the Agreement, a valid legal basis and (where applicable) condition for the Processing by Crunchy Data of Customer Personal Data in accordance with this Data Processing Addendum and the Agreement (including, any and all instructions issued by Customer from time to time in respect of such Processing).

3. SUPPLIER PERSONNEL

Crunchy Data shall take reasonable steps to ensure the reliability of any Crunchy Data Personnel who Process Customer Personal Data, ensuring**:**

(a) that access is strictly limited to those individuals who need to know or access the relevant Customer Personal Data for the purposes described in this Data Processing Addendum; and

(b) that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. SECURITY

4.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk (which may be of varying likelihood and severity) for the rights and freedoms of natural persons, Crunchy Data shall implement appropriate technical and organisational measures in relation to Customer Personal Data to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2. In assessing the appropriate level of security, Crunchy Data shall take account in particular of the risks presented by the Processing, in particular from a Personal Data Breach.

4.3. Without limiting the generality of Paragraphs 4.1 and 4.2, Crunchy Data shall endeavour to comply with the Security Measures set out in Annex 3.

5. SUBPROCESSING

5.1. Customer authorises Crunchy Data to appoint Subprocessors in accordance with this Paragraph 5.

5.2. Crunchy Data may continue to use those Subprocessors already engaged by Crunchy Data as at the date of this Data Processing Addendum, subject to Crunchy Data meeting within a reasonable timeframe (or having already met) the obligations set out in Paragraph 5.4.

5.3. Crunchy Data shall give Customer prior written notice of the appointment of any proposed Subprocessor, including reasonable details of the Processing to be undertaken by the Subprocessor. If, within fourteen (14) days days of receipt of that notice, Customer notifies Crunchy Data in writing of any objections (on reasonable grounds) to the proposed appointment:

(a) Crunchy Data shall use reasonable efforts to make available a commercially reasonable change in the provision of the Services, which avoids the use of that proposed Subprocessor; and

(b) where:

(i) such a change cannot be made within fourteen (14) days days from Crunchy Data receipt of Customer's notice;

(ii) no commercially reasonable change is available; and/or

(iii) Customer declines to bear the cost of the proposed change,

either party may by written notice to the other party with immediate effect terminate the Agreement either in whole or to the extent that it relates to the Services which require the use of the proposed Subprocessor.

5.4. With respect to each Subprocessor, Crunchy Data shall ensure that the arrangement between Crunchy Data and the Subprocessor is governed by a written contract including terms which offer at least an equivalent level of protection for Customer Personal Data as those set out in this Data Processing Addendum (including those set out in Paragraph 4).

6. DATA SUBJECT RIGHTS

6.1. Taking into account the nature of the Processing, Crunchy Data shall provide Customer with such assistance as may be reasonably necessary and technically possible in the circumstances, to assist Customer in fulfilling its obligation to respond to Data Subject Requests.

6.2. Crunchy Data shall:

(a) promptly notify Customer if it receives a Data Subject Request; and

(b) ensure that it does not respond to any Data Subject Request except on the written instructions of Customer (and in such circumstances, at Customer's cost) or as required by applicable laws.

7. PERSONAL DATA BREACH

7.1. Crunchy Data shall notify Customer without undue delay upon Crunchy Data becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information (insofar as such information is, at such time, within Crunchy Data's possession) to allow Customer to meet any obligations under the GDPR to report the Personal Data Breach to:

(a) affected Data Subjects; or

(b) the relevant Supervisory Authority(ies) (as may be determined in accordance with the GDPR).

7.2. Crunchy Data shall co-operate with Customer and take such reasonable commercial steps as may be directed by Customer to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

Crunchy Data shall provide reasonable assistance to Customer, at Customer's cost, with any data protection impact assessments, and prior consultations with Supervisory Authorities, which Customer reasonably considers to be required of it by Article 35 or Article 36 of the GDPR, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing by, and information available to, Crunchy Data.

9. DELETION OR RETURN OBLIGATIONS

9.1 Subject to Paragraphs 9.2 and 9.5, upon the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), Crunchy Data shall immediately cease all Processing of the Customer Personal Data for any purpose other than for storage.

9.2 Subject to Paragraph 9.5, to the extent technically possible in the circumstances (as determined in Crunchy Data's sole discretion), on written request to Crunchy Data (to be made no later than fourteen (14) days after the Cessation Date ("**Post-cessation Storage Period**")), Crunchy Data shall:

(a) return a complete copy of all Customer Personal Data within Crunchy Data's possession to Customer by secure file transfer, promptly following which Crunchy Data shall Delete all other copies of such Customer Personal Data; or

(b) Delete all Customer Personal Data then within Crunchy Data's possession.

9.3 Crunchy Data shall comply with any written request made pursuant to Paragraph 9.2 within thirty (30) days thereof.

9.4 In the event that during the Post-cessation Storage Period, Customer does not instruct Crunchy Data in writing to either Delete or return the Customer Personal Data pursuant to Paragraph 9.2, Crunchy Data shall promptly after the expiry of the Post-cessation Storage Period Delete all Customer Personal Data then within Crunchy Data's possession to the fullest extent technically possible in the circumstances.

9.5 Crunchy Data and any Subprocessor may retain Customer Personal Data where required by applicable law, for such period as may be required by such applicable law, provided that Crunchy Data and any such Subprocessor shall ensure:

(a) the confidentiality of all such Customer Personal Data; and

(b) that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in the applicable law requiring its storage and for no other purpose.

10. AUDIT RIGHTS

10.1. Crunchy Data shall make available to Customer on request such information as Crunchy Data (acting reasonably) considers appropriate in the circumstances to demonstrate its compliance with this Data Processing Addendum.

10.2. Subject to Paragraphs 10.3 and 10.4, in the event that Customer (acting reasonably) is able to provide documentary evidence that the information made available by Crunchy Data pursuant to Paragraph 10.1 is not sufficient in the circumstances to demonstrate Crunchy Data’s compliance with this Data Processing Addendum, Crunchy Data shall allow for and contribute to audits, including on-premise inspections, by Customer or an auditor mandated by Customer in relation to the Processing of the Customer Personal Data by Crunchy Data.

10.3. Customer shall give Crunchy Data reasonable notice of any audit or inspection to be conducted under Paragraph 10.1 (which shall in no event be less than fourteen (14) days’ notice unless required by a Supervisory Authority pursuant to Paragraph 10.4(f)) and shall use its best efforts (and ensure that each of its mandated auditors uses its best efforts) to avoid causing, any damage, injury or disruption to Crunchy Data’s premises, equipment, Personnel, data, and business (including any interference with the confidentiality or security of the data of Crunchy Data’s other customers or the availability of Crunchy Data’s services to such other customers) while its Personnel and/or its auditor’s Personnel (if applicable) are on those premises in the course of any on-premise inspection.

10.4. Crunchy Data need not give access to its premises for the purposes of such an audit or inspection:

(a) to any individual unless he or she produces reasonable evidence of their identity and authority;

(b) to any auditor whom Crunchy Data has not given its prior written approval (not to be unreasonably withheld);

(c) unless the auditor enters into a non-disclosure agreement with Crunchy Data on terms acceptable to Crunchy Data;

(d) where, and to the extent that, Crunchy Data considers, acting reasonably, that to do so would result in interference with the confidentiality or security of the data of Crunchy Data’s other customers or the availability of Crunchy Data’s services to such other customers;

(e) outside normal business hours at those premises; or

(f) on more than one occasion in any calendar year during the term of the Agreement, except for any additional audits or inspections which Customer is required to carry out under the GDPR or by a Supervisory Authority, where Customer has identified the relevant requirement in its notice to Crunchy Data of the audit or inspection.

10.5. The Parties shall discuss and agree the costs of any inspection or audit to be carried out by or on behalf of Customer pursuant to this Paragraph 10.4 in advance of such inspection or audit and, unless otherwise agreed in writing between the Parties, Customer shall bear any third party costs in connection with such inspection or audit and reimburse Crunchy Data for all costs incurred by Crunchy Data and time spent by Crunchy Data (at Crunchy Data’s then-current professional services rates) in connection with any such inspection or audit.

11. RESTRICTED TRANSFERS

11.1. Subject to Paragraph 11.2, to the extent that any Processing by either Crunchy Data or any Subprocessor of Customer Personal Data involves a Restricted Transfer, the Parties agree that:

(a) Customer – as “data exporter”; and

(b) Crunchy Data or Subprocessor (as applicable) – as “data importer”,

shall enter into the Standard Contractual Clauses in respect of that Restricted Transfer and the associated Processing in accordance with Paragraph 11.2.

11.2. The Standard Contractual Clauses shall be deemed to come into effect under Paragraph 11.1 automatically upon the commencement of the relevant Restricted Transfer **provided that** Paragraph 11.1 shall not apply to a Restricted Transfer unless its effect is to allow the relevant Restricted Transfer and the associated Processing to take place without breach of the GDPR.

11.3. In relation to any Restricted Transfer requiring a transfer mechanism under Chapter V of the UK GDPR – for the purposes of the UK GDPR only, the Standard Contractual Clauses entered into pursuant to this Paragraph 11 are hereby deemed to be amended to reflect the version of those Standard Contractual Clauses issued and published by the UK ICO that reflect variations:

(a) required to account for the specific requirements of the UK GDPR; and

(b) permitted by paragraph 7 of Schedule 21 to the DPA 2018,

which as at the date hereof, are as shown at https://ico.org.uk/media/for-organisations/documents/2618973/uk-sccs-c-p-202012.docx/.

12. INCORPORATION AND PRECEDENCE

12.1. This Data Processing Addendum is hereby incorporated into and forms part of the Agreement with effect from the Addendum Effective Date.

12.2. In the event of any conflict or inconsistency between:

(a) this Data Processing Addendum and the Agreement, this Data Processing Addendum shall prevail; or

(b) any Standard Contractual Clauses entered into pursuant to Paragraph 11 and this Data Processing Addendum and/or the Agreement, those Standard Contractual Clauses shall prevail **provided that**, it is agreed that the following shall apply:

(i) in the event of any request under Clause 5(j) of the Standard Contractual Clauses that Crunchy Data provide copies of any Subprocessor agreement(s) to the Customer, Crunchy Data may remove or redact all commercial information or all or part of any clauses, recitals, schedules annexes, appendices etc., unrelated to the Standard Contractual Clauses or their equivalent beforehand;

(ii) the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be performed in accordance with Paragraph 10, and shall be subject to any relevant conditions, limitations or restrictions therein;

(iii) any authorisations or approvals of current and future Subprocessors given to Crunchy Data pursuant to Paragraph 5 will constitute Customer’s prior written consent to the subcontracting by Crunchy Data of the Processing of Customer Personal Data if and as such consent is required under Clause 5(h) of the Standard Contractual Clauses; and

(iv) certification of deletion of Customer Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided only upon Customer’s written request.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

Annex 1 Data Processing Details

This Annex 1 includes certain details of the Processing of Customer Personal Data: as required by Article 28(3) GDPR.

Crunchy Data's activities

Crunchy Data provides a fully managed PostgreSQL offering hosted on top of cloud infrastructure – whose operations include the provision of the relevant Crunchy Data Service(s) to Customer, and certain associated Processing of Customer Personal Data on Customer's behalf, subject to and in accordance with the Data Processing Addendum and/or the Agreement.

Subject matter and duration of the Processing of Customer Personal Data

The subject matter and duration of the Processing of the Customer Personal Data are set out in the Agreement and the Data Processing Addendum.

The nature and purpose of the Processing of Customer Personal Data

The purpose of the Processing of the Customer Personal Data under this Data Processing Addendum is the provision of the Crunchy Data Service(s) initiated by Customer from time to time as set out in the Agreement and the Data Processing Addendum.

The types of Customer Personal Data to be Processed

Customer Personal Data uploaded to the Crunchy Data Service(s) initiated by Customer from time to time, as determined by Customer in its sole discretion.

The categories of Data Subject to whom the Customer Personal Data relates

The data subjects may include Customer's customers, personnel (including employees, consultants and contractors), suppliers and end-users.

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Agreement and the Data Processing Addendum.

Annex 2 Controller-to-Processor Standard Contractual Clauses

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

> Customer, whose particulars are set out in the pre-amble to the Addendum to which these Standard Contractual Clauses are attached (the **data exporter**)
>
> Crunchy Data, whose particulars are set out in the pre-amble to the Addendum to which these Standard Contractual Clauses are attached (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;

(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 subprocessor”* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor 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

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 subprocessing, 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent;

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

(j) to send promptly a copy of any subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor 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 subprocessor, 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 subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, 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 laws of the jurisdiction in which the data exporter is established.

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

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor 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 subprocessor’s obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the laws of the jurisdiction in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing 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 subprocessor 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 subprocessor 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.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data exporter	Customer, who is a party to the Data Processing Addendum to which these Standard Contractual Clauses are attached. Customer is a customer of certain Crunchy Data Service(s), and the EEA-based entity on whose behalf Customer Personal Data will be Processed in the context of Crunchy Data's provision of those relevant Crunchy Data Service(s) subject to and in accordance with the Data Processing Addendum and/or the Agreement.
Data importer	Crunchy Data Solutions, Inc., whose particulars are set out in the pre-amble to the Data Processing Addendum to which these Standard Contractual Clauses are attached. Crunchy Data provides a fully managed PostgreSQL offering hosted on top of cloud infrastructure – whose operations include the provision of the relevant Crunchy Data Service(s) to Customer, and certain associated Processing of Customer Personal Data on Customer's behalf, subject to and in accordance with the Data Processing Addendum and/or the Agreement.
Data Subjects	As described in Annex 1 to the Data Processing Addendum to which these Standard Contractual Clauses are attached.
Categories of Data	As described in Annex 1 to the Data Processing Addendum to which these Standard Contractual Clauses are attached.
Special categories of data	As described in Annex 1 to the Data Processing Addendum to which these Standard Contractual Clauses are attached.
Processing Operations	Any Processing of Customer Personal Data carried out by Crunchy Data on behalf of the Customer, which is part of Crunchy Data's provision of the relevant Crunchy Data Service(s) to the Customer subject to and in accordance with the Data Processing Addendum and/or the Agreement.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

The technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) are those established and maintained under Paragraph 4 of the Data Processing Addendum (including the Security Measures set out in Annex 3).

crunchy data

Annex 3 Security Measures

As from the Addendum Effective Date, Crunchy Data will implement and maintain the security measures set out in this Annex 3 ("**Security Measures**").

1. Organisational management and dedicated staff responsible for the development, implementation and maintenance of Crunchy Data's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Crunchy Data's organisation, monitoring and maintaining compliance with Crunchy Data's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Personal Data that is:

(a) transmitted over public networks (i.e. the Internet) or when transmitted wirelessly; or

(b) at rest or stored on portable or removable media (i.e. laptop computers, CD/DVD, USB drives, back-up tapes).

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access when employment terminates or changes in job functions occur).

5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Crunchy Data passwords that are assigned to its employees must:

(a) be at least eight (8) characters in length;

(b) not be stored in readable format on Crunchy Data's computer systems;

(c) have defined complexity; and

(d) if newly-issued, be changed after first use.

6. Physical and environmental security of data centre, server room facilities and other areas containing Personal Data designed to:

(a) protect information assets from unauthorised physical access,

(b) manage, monitor and log movement of persons into and out of Crunchy Data facilities, and

(c) guard against environmental hazards such as heat, fire and water damage.

7. Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Crunchy Data's technology and information assets.

8. Incident / problem management procedures designed to allow Crunchy Data to investigate, respond to, mitigate and notify of events related to Crunchy Data's technology and information assets.

9. Network security controls that provide for the use of enterprise firewalls, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

10. Vulnerability assessment and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

11. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Crunchy Data may update or modify such Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services.