DS
CL

Couchbase

Couchbase Enterprise Customer Data Processing Addendum

This Data Processing Addendum (this "**DPA**") amends the terms and forms part of the Enterprise Subscription License Agreement, or other agreement between Customer and Couchbase governing Customer's use of the Services ("**Agreement**"), between Couchbase, Inc. ("**Couchbase**") and the party identified as the "Customer" in the Agreement ("**Customer**") (each a "**Party**" and together, the "**Parties**"). By executing this DPA, Customer enters into this DPA on behalf of itself and in the name and on behalf of its Affiliates, if and to the extent Couchbase processes Personal Data for which such Affiliates qualify as the Controller.

This DPA describes the commitments of the Parties concerning the processing of Personal Data in connection with Customer's use of the Services. If there is any conflict between the terms of the Agreement and the terms of this DPA, the terms of this DPA shall prevail to the extent of such conflict. Any capitalized term not defined in this DPA will have the meaning given it in the Agreement.

HOW TO COMPLETE THIS DPA:

For this DPA to be effective between the Parties, Customer must:

1. Download this DPA for completion;
2. Fill in the information requested in the signature block and any other area requiring Customer's information; and
3. Return the signed DPA to Couchbase by email at legal@couchbase.com, indicating Customer's full legal name and whether Customer is a current or prospective customer of Couchbase.
4. This DPA (including any attachments) will not become effective until (i) Couchbase acknowledges receipt of the fully signed DPA received at the above alias; and (ii) the Parties have entered into an effective Agreement for Couchbase's products and services (the date on which such conditions are met, the "**Effective Date**").

The Parties agree as follows:

1. **Definitions.** The following capitalized terms, when used in this DPA, will have the corresponding meanings provided below:

   a) "**Affiliate**" means any entity that directly, or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party. For purposes of this definition, the term "control" means the power (or, as applicable, the possession or exercise of the power) to direct, or cause the direction of, the management, governance, or policies of a given entity, directly or indirectly, through any applicable means (whether through the legal, beneficial, or equitable ownership, of more than fifty percent (50%) of the aggregate of all voting or equity interests or securities of such entity, through partnership, or through some other form of ownership interest, by contract, or other applicable legal document, or otherwise).

   b) "**Applicable Data Protection Laws**" means all worldwide privacy and data protection laws, regulations, rules, ordinances and other decrees applicable to the Personal Data, including (but not limited to): (i) European Data Protection Laws; and (ii) all laws and regulations of the United States, including the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq) (*"***CCPA***"*); as may be amended, superseded or replaced.

c) "**Customer Data**" means any Personal Data processed by Couchbase on behalf of Customer as a service provider or processor (as applicable) in connection with the Services, as more particularly described in Annex C of this DPA.

d) "**EEA**" means the Member States of the European Union, plus Iceland, Liechtenstein, Norway and the United Kingdom until the European Union law ceases to apply.

e) "**European Data Protection Laws**" means: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**"); (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector ("**e-Privacy Directive**"); (iii) any applicable national implementations of (i) and (ii); (iv) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance (the "**Swiss DPA**"); and (v) in respect of the United Kingdom, the Data Protection Act 2018 and any applicable national legislation that replaces or converts in domestic law the GDPR (the "**UK GDPR**"), e-Privacy Directive or any other law relating to data and privacy as a consequence of the UK leaving the European Union; in each case as may be amended, superseded or replaced.

f) "**Personal Data**" means any information that relates to an identified or identifiable natural person and which is protected as "personal data", "personal information" or "personally identifiable information" under Applicable Data Protection Laws.

g) "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data transmitted, stored or otherwise processed by Couchbase and/or its Sub-processors in connection with the provision of the Services. The Parties acknowledge and agree that "Security Incident" shall not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems, or any breach of security caused by Customer.

h) "**Services**" means any Couchbase services and products provided to Customer pursuant to the Agreement.

i) "**Standard Contractual Clauses**" means (i) where the GDPR applies the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (the "EU SCCs"); and (ii) where the Swiss DPA applies, the applicable standard data protection clauses issued, approved or otherwise recognized by the Swiss Federal Data Protection and Information Commissioner (the "Swiss SCCs").

j) "**Sub-processor**" means any processor engaged by Couchbase or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA. Sub-processors may include third parties or Couchbase Affiliates but shall exclude any Couchbase employee, contractor or consultant.

k) "**UK IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, where Couchbase is Processor and Customer is Controller.

l) The terms "**controller**", "**processor**" and **"processing**" shall have the meanings given to them in the GDPR, and "**process**", "**processes**" and "**processed**" shall be interpreted accordingly; and the terms "**business**", "**service provider**" and "**sell**" shall have the meanings given to them in the CCPA.

2. Role and Scope of Processing

a) **Scope.** This DPA applies to the extent that Couchbase processes as a processor or service provider (as applicable) any Customer Data protected by Applicable Data Protection Laws.

b) **Role of the Parties.** The parties acknowledge and agree that (i) Customer is a business or the controller (as applicable) with respect to the processing of Customer Data, and Couchbase shall process Customer Data only as a processor or service provider (as applicable) on behalf of Customer, as further described in Annex C of this DPA and (ii) Couchbase may process Personal Data, including business contact information, as the relevant business or independent controller for its own legitimate business purposes in accordance with the Couchbase privacy policy available at https://www.couchbase.com/privacy-policy, updated from time to time. Each Party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including any Applicable Data Protection Laws.

c) **Couchbase processing of Customer Data.** Couchbase agrees that it shall process Customer Data only for the purposes described in the DPA and in accordance with Customer's documented lawful instructions. The parties agree that the Agreement (including this DPA) sets out the Customer's complete and final instructions to Couchbase in relation to the processing of Customer Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Couchbase. Without prejudice to Section 2(d) (Customer responsibilities), Couchbase shall notify Customer in writing, unless prohibited from doing so under Applicable Data Protection Laws, and may suspend processing of Customer Data, if it becomes aware or believes that any data processing instructions from Customer violates Applicable Data Protection Laws.

d) **Customer responsibilities.** Customer is responsible for the lawfulness of Customer Data processing under or in connection with the Agreement. Customer represents and warrants that (i) it has provided, and will continue to provide all notice and obtained, and will continue to obtain, all consents, permissions and rights necessary under Applicable Data Protection Laws for Couchbase to lawfully process Customer Data for the purposes contemplated by the Agreement (including this DPA); (ii) it has complied with all Applicable Data Protection Laws as a controller and/or business of Customer Data for the collection and provision to Couchbase and its Sub-processors of such Customer Data; and (iii) it shall ensure its processing instructions comply with applicable laws (including Applicable Data Protection Laws) and that the processing of Customer Data by Couchbase in accordance with Customer's instructions will not cause Couchbase to be in breach of Applicable Data Protection Laws.

e) **Aggregate data.** Notwithstanding the foregoing or anything to the contrary in the Agreement (including this DPA), Customer acknowledges that Couchbase and its Affiliates shall have a right to collect and create anonymized, aggregate, and/or de-identified information (as defined by Applicable Data Protection Laws) for its own legitimate business.

3. Subprocessing

a) Authorized Sub-processors. Customer acknowledges and agrees that Couchbase may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by Couchbase and authorized by Customer are listed in Annex D. Customer may request that Couchbase inform Customer of any changes regarding such Sub-processors.

4. Security and Audits

a) Security Measures. Couchbase shall implement and maintain appropriate technical and organizational security measures designed to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing ("**Security Measures**"). Such Security Measures will include, at a minimum, those measures described in Annex D of this DPA. Couchbase shall ensure that any person who is authorized by Couchbase to process Customer Data under this DPA shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

b) **Updates to Security Measures**. Customer acknowledges that the Security Measures are subject to technical progress and development and that Couchbase may update or modify the 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 purchased by the Customer.

c) **Customer Security Responsibilities**. Notwithstanding the above, Customer agrees that except as provided by this DPA, Customer shall implement and maintain appropriate technical and organizational security measures designed to protect Personal Data from Security Incidents and to preserve the security and confidentiality of Customer Data while in its dominion and control. Customer is responsible for, as applicable to the Agreement, protecting the security of all Customer credentials used to access the Services; (ii) securing any Customer System (with such steps to include without limitation the regular rotation of access keys and other industry standard steps to preclude unauthorized access); and (iii) backing up and securing Customer Data under Customer's control within any Customer controlled system.

d) **Security Incident Response**. To the extent required by Applicable Data Protection Laws, upon becoming aware of a Security Incident, Couchbase shall notify Customer without undue delay and shall: (i) to assist Customer in relation to any Personal Data breach notifications Customer is required to make under Applicable Data Protection Laws, Couchbase will include in such notice to Customer timely information relating to the Security Incident as it becomes known, as is reasonably requested by Customer, taking into account the nature of the Services, the information available to Couchbase, and any restrictions on disclosing the information, such as confidentiality; and (ii) promptly take steps, deemed necessary and reasonable by Couchbase, to contain, investigate, and remediate any Security Incident, to the extent that the remediation is within Couchbase's reasonable control. Couchbase's notification of or response to a Security Incident under this Section 4(d) shall not be construed as an acknowledgment by Couchbase of any fault or liability with respect to the Security Incident. The obligations set forth herein shall not apply to Security Incidents to the extent they are caused by Customer or its Authorized Users.

e) **Security Audits.** Couchbase shall provide written responses (on a confidential basis) to all reasonable written requests for information made by Customer related to Couchbase's processing of Customer Data, including responses to information security and audit questionnaires that are necessary to confirm Couchbase's compliance with this DPA, provided that Customer shall not exercise this right more than once in any twelve (12) month rolling period. Notwithstanding the foregoing, Customer may also exercise such audit right in the event Customer is expressly requested or required to provide this information to a data protection authority, or Couchbase has experienced a Security Incident, or on another reasonably similar basis.

5. International Transfers

a) **Processing locations.** Customer acknowledges and agrees that Couchbase may transfer and process Customer Data to and in the United States and anywhere else in the world where Couchbase, its Affiliates or its Sub-processors maintain data processing operations. Couchbase shall at all times ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws and this DPA, including the provisions of Section 8 below regarding transfers.

6. Deletion of Customer Data

a) The Services will provide Customer with controls that Customer may use to delete or retrieve Customer Data during the term in a manner consistent with the functionality of the Services.

b) Upon termination or expiry of the Agreement, on Customer's request, Couchbase shall delete all Customer Data (including copies) in its possession or control in accordance with the Agreement, save that this requirement shall not apply to the extent Couchbase is required by applicable law to retain some or all of the Customer Data.

7. Rights of Individuals and Cooperation

a) **Data Subject Requests.** The Services provide Customer with a number of controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Customer Data, as described in any documentation applicable to the Services. Without prejudice to Section 4(a), Customer may use these controls as technical and organizational measures to assist it in connection with its obligations under Applicable Data Protection Laws, including its obligations relating to responding to requests from data subjects. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, Couchbase shall, taking into account the nature of the processing, provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Customer Data under the Agreement. In the event that any such request is made to Couchbase directly, Couchbase shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Couchbase is required to respond to such a request, Couchbase shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

b) **Subpoenas and Court Orders**. If a law enforcement agency sends Couchbase a demand for Customer Data (for example, through a subpoena or court order), Couchbase shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Couchbase is legally prohibited from doing so.

8. Jurisdiction Specific Terms

a) **Europe.** To the extent the Customer Data is subject to European Data Protection Laws, the following terms shall apply in addition to the terms in the remainder of this DPA:

1. Sub-processor Obligations. Couchbase shall: (A) enter into a written agreement with each Sub-processor imposing data protection terms that require the Sub-processor to protect Personal Data to the standard required by applicable European Data Protection Law and this DPA; and (B) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Couchbase to breach any of its obligations under this DPA.
2. Objections to Sub-processors. Customer may object in writing to Couchbase’s appointment of a new Sub-processor on reasonable grounds relating to data protection (e.g. if making Customer Data available to the Sub-processor may violate European Data Protection Law or weaken the protections for such Customer Data) by notifying Couchbase promptly in writing within five (5) calendar days of receipt of notice from Couchbase in accordance with Section 3(a) above. Such notice shall explain the reasonable grounds for the objection and the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If no such resolution can be reached, Couchbase will, at its sole discretion, either not appoint Sub-processor, or permit Customer to suspend or terminate the affected Service in accordance with the

termination provisions in the Agreement without liability to either party (but without prejudice to any fees incurred by Customer prior to suspension or termination). Unless an objection is made as set forth in this Section 8(a)(ii), Customer consents to Couchbase's use of sub-processors as described in this DPA.

3. Transfers of Data. To the extent that Couchbase processes (or causes to be processed) any Personal Data protected by European Data Protection Laws in a third country not recognized as providing adequate protection for Personal Data (as described in European Data Protection Laws), then the Parties will be deemed to have entered into (i) as to any transfers from the European Economic Area and/or Switzerland, the Standard Contractual Clauses with Couchbase (as data importer) as set forth in Annex A; and (ii) as to any transfers from the United Kingdom, the UK IDTA as set forth in Annex B and Couchbase agrees to abide by and process such Customer Data in compliance with the Standard Contractual Clauses and the UK IDTA, which are incorporated in full by reference and form an integral part of this DPA. Annexes C, D, and E hereto are incorporated as the applicable appendices to the Standard Contractual Clauses and the UK IDTA. It is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Standard Contractual Clauses or the UK IDTA. Accordingly, if and to the extent the Standard Contractual Clauses or the UK IDTA conflict with any provision of this DPA, the Standard Contractual Clauses or the UK IDTA shall prevail to the extent of such conflict. The Standard Contractual Clauses and/or the UK IDTA will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA, Switzerland or the United Kingdom.
4. Alternative Transfer Mechanism. If and to the extent that Couchbase adopts an alternative data export solution for the transfer of Customer Data as prescribed by applicable European Data Protection Laws ("**Alternative Transfer Mechanism**"), the Alternative Transfer Mechanism shall apply instead (but only to the extent such Alternative Transfer Mechanism applies to the transfer).
5. Data Protection Impact Assessment. To the extent Couchbase is required under applicable European Data Protection Law, Couchbase shall provide reasonably requested information regarding Couchbase processing of Personal Data under the Agreement to enable the Customer to carry out data protection impact assessments or prior consultations with supervisory authorities as required by law.

b) **California.** To the extent the Customer Data is subject to the CCPA, the parties agrees that Customer is a business and that it appoints Couchbase as its service provider to process Customer Data as permitted under the Agreement (including this DPA) and the CCPA, or for purposes otherwise agreed in writing (the "**Permitted Purposes**"). Customer and Couchbase agree that: (i) Couchbase shall not retain, use or disclose personal information for any purpose other than the Permitted Purposes; (ii) Customer Data was not sold to Couchbase and Couchbase shall not "sell" personal information (as defined by the CCPA); (iii) Couchbase shall not retain, use or disclose personal information outside of the direct business relationship between Customer and Couchbase; and (iv) Couchbase may de-identify or aggregate personal information in the course of providing the Services. Couchbase certifies that it understands the restrictions set out in this Section 8(b) and will comply with them.

9. Limitation of Liability

a) Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA (including the Standard Contractual Clauses) whether in contract, tort (including negligence) or under any other theory of liability, shall be subject to the limitations and exclusions of liability in the Agreement, and any reference in provisions to the liability of a party means the aggregate liability of that party and all of its Affiliates under and in connection with the Agreement and this DPA together.

b) Except where Applicable Data Protection Laws require a Customer Affiliate to exercise a right or seek any remedy under this DPA against Couchbase directly by itself, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement shall exercise any right or seek any remedy any Customer Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Affiliate individually but in a combined manner for all of its Affiliates together.

10. Miscellaneous

a) Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect.

b) This DPA may be executed in counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

c) If any provision or part-provision of this DPA is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of the DPA.

d) This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Agreement, unless required otherwise by European Data Protection Laws.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative and this DPA shall be effective on the date both parties sign this DPA:

Customer (Required):	**Couchbase**
	DocuSigned by: Bill Carey 85619C3A810748E...
By (Required):________________________	By: BILL CAREY ________________________
Title (Optional):______________________	Title: VP Controller ______________________
Date (Required):______________________	Date: December 21, 2022 ____________________

Annex A

Standard Contractual Clauses

SECTION I

Clause 1

Purpose and scope

(a)The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b)The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

[Intentionally Blank]

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject’s prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

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

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

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

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6] (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

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

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

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

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

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

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

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

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

MODULE THREE: Transfer processor to processor

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

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

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

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

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

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

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

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

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

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

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

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

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

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

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

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

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

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

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

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

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

Clause 15

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

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

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

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

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of another EU Member State mutually agreed upon by both Parties.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of another EU Member STate mutually agreed upon by both Parties.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the EU Member State of which the data exporter is established.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Annex B

UK IDTA

The Parties agree:

1. The provisions of the UK IDTA, including Part 2 ‘Mandatory Clauses’, shall apply in full;

2. For the purposes of Table 1 of the UK IDTA, the names of the parties, their roles and their details shall be set out in Annex C;

3. For the purposes of Tables 2 and 3 of the UK IDTA, the Standard Contractual Clauses incorporated into this DPA as Annex A, including the information set out in the attached Annexes, shall apply; and

4. For the purposes of Table 4 of the UK IDTA, either party may end the UK IDTA if, after a good faith effort by the parties to amend this DPA, the parties are unable to come to a mutual agreement.

Annex C

Data Processing Description

This Annex C forms part of the DPA and describes the processing that Couchbase will perform on behalf of the Customer as well as describes the transfer of any Personal Data under the DPA.

Section IA. List of Parties

Data exporter:

Name: As set out on the signature page of the DPA

Address: As set out on the signature page of the DPA

Contact person's name, position and contact details: Customer's main point of contact

Activities relevant to the data transferred under these Clauses: Receipt of database products and services

Signature and date: As set out on the signature page of the DPA

Role (controller/processor): Controller or Processor, as applicable

Data Importer:

1. Name: Couchbase, Inc.

Address: 3250 Olcott Street, Santa Clara CA 95054 USA

Contact person's name, position and contact details: legal@couchbase.com

Activities relevant to the data transferred under these Clauses: Provision of database products and services

Signature and date: As set out on the signature page of the DPA

Role (controller/processor): Processor or Controller, as applicable

Section 1B. Description of Transfer

Controller to Processor / Processor to Processor

Duration and Retention

The duration of the data processing (and transfers, if applicable) under this DPA is until the termination of the Agreement in accordance with its terms plus the period from the expiry of the Agreement until deletion of Personal Data by Couchbase in accordance with the terms of the Agreement.

Frequency of the Transfer

When initiated, transfers of Personal Data may be continuous.

Categories of data

The Personal Data to be processed (and transferred, if applicable) concern the following categories of data (please specify):

- Personal Data included in content or data provided by or on behalf of Customer or Authorized Users by or through the Services, including in connection with any Support.

Special categories of data (if appropriate)

The parties do not intend for any special category data to be processed or transferred under the Agreement.

Data subjects

The Personal Data to be processed (and transferred, if applicable) concern the following categories of data subjects (please specify):

- Data subjects include individuals about whom data is provided to Couchbase via the Services by or at the direction of Customer, including Authorized Users. Data subjects may include Customer’s customers, employees, suppliers and end-users.

Processing operations

The Personal Data will be subject to the following basic processing activities and any transfers are for the following purposes (please specify):

- processing to provide the Services in accordance with the Agreement
- processing to perform any steps necessary for the performance of the Agreement
- processing initiated by Customer in its use of the Services
- processing to comply with other reasonable instructions provided by Customer (e.g. via email or support tickets) that are consistent with the terms of this Agreement.

Controller to Controller

Retention

Couchbase retains Personal Data it processes as a controller for as long as required for its legitimate business purposes, determined by whether Couchbase has a legal obligation to retain the Personal Data and the length of time of Couchbase’s business relationship with a customer.

Frequency of the Transfer

When initiated, transfers of Personal Data may be continuous.

Categories of data

The Personal Data to be processed (and transferred, if applicable) concern the following categories of data (please specify):

- Customer employee and authorized user contact information, which may include name, company name, role, email and phone number; and
- Employee and authorized user usage information, which may include location and IP address.

Special categories of data (if appropriate)

The parties do not intend for any special category data to be processed or transferred under the Agreement.

Data subjects

The Personal Data to be processed (and transferred, if applicable) concern the following categories of data subjects (please specify):

- Customer's employees and authorized users.

Processing operations

The Personal Data will be processed for Couchbase's legitimate business purposes and subject to the following basic processing activities and any transfers are for the following purposes (please specify):

- Billing, account and customer relationship management and related correspondence with customers;
- Complying with and resolving legal obligations; and
- Product and service improvement.

Section 1C. Competent Supervisory Authority

The data protection authorities of the locations of which the data exporter is established.

Annex D

Security Measures

This Annex describes Couchbase's Security Measures in providing the Services. Customer acknowledges that the Service operates pursuant to a shared responsibility model, which requires, among other things, that Customer take certain steps such as protecting the security of any Customer environment into which Couchbase products are deployed. If and to the extent Couchbase processes Customer Data on behalf of Customer in connection with the Service, Couchbase shall implement and maintain the following Security Measures:

1. **System Access Controls**: Couchbase shall take reasonable measures to prevent unauthorized use of the systems used for processing Customer Data. These controls shall vary based on the nature of the processing undertaken and may include, among other controls, strong authentication, documented authorization processes, documented change management processes and/or, logging of access on several levels.
2. **Data Access Controls**: Couchbase shall take reasonable measures to provide that any Customer Data in Couchbase's control is accessible and manageable only by properly authorized staff. Application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Customer Data to which they have access privileges; and, that Customer Data cannot be read, copied, modified or removed without authorization in the course of processing.
3. **Transmission Controls**: Couchbase shall take reasonable measures to ensure that Customer Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport. Couchbase uses industry standard firewall and encryption technologies to protect data in transit and at rest.
4. **Input Controls**: Couchbase shall take reasonable measures to provide that it is possible to check and establish whether and by whom Customer Data has been entered into data processing systems, modified or removed; and, any transfer of Customer Data to a third-party service provider is made via a secure transmission.
5. **Data Protection**: Couchbase shall take reasonable measures to ensure that Customer Data is protected against accidental destruction or loss.
6. **Logical Separation**: Customer Data in Couchbase's control is logically segregated on systems managed by the Couchbase to prevent unauthorized access.

Annex E

List of Affiliates and Subprocessors

To provide the products and services licensed by Customer under the Agreement, Couchbase may engage the Couchbase Affiliates, Infrastructure Providers, and Other Third-Party Subprocessors as disclosed at https://info.couchbase.com/cloud-subprocessors.html.