MongoDB Data Processing Agreement

This Data Processing Agreement (**"DPA"**) is incorporated into and forms a part of the Cloud Subscription Agreement, Cloud Terms of Service, or other applicable service or subscription agreement between you and MongoDB with respect to your use of the Cloud Services (**"MongoDB Agreement"**). This DPA sets out data protection requirements with respect to the processing of Customer Personal Data (as defined below) that is collected, stored, or otherwise processed by MongoDB for the purpose of providing the Cloud Services. This DPA is effective on the effective date of the MongoDB Agreement, unless this DPA is separately executed in which case it is effective on the date of the last signature.

1. Definitions.

The following terms have the following meanings when used in this DPA. Any capitalized terms that are not defined in this DPA have the meaning provided in your MongoDB Agreement.

"**California Consumer Privacy Act of 2018**" or **"CCPA"** means the California Consumer Privacy Act of 2018, as may be amended from time to time.

"**Customer**," "**you**" and "**your**" means the organization that agrees to an Order Form, or uses the Cloud Services subject to the relevant MongoDB Agreement.

"**Customer Personal Data**" means any personal data that Customer uploads into the Cloud Services that is processed by MongoDB.

"**Data Protection Law**" means GDPR, CCPA, and any other data protection legislation applicable to the respective party in its role in the processing of Customer Personal Data under the MongoDB Agreement.

"**Data Subject Request**" has the meaning given to it in Section 5.1.

"**EEA**" means the European Economic Area.

"**GDPR**" means the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended, updated or replaced from time to time, in the European Union, Switzerland and/or the United Kingdom.

"**Standard Contractual Clauses**" means the Standard Contractual Clauses for Processors as approved by the European Commission in the form set out in Annex 1.

"**Subprocessor**" means any third-party data processor engaged by MongoDB to process Customer Personal Data.

"**Technical and Organizational Security Measures**" has the meaning given to it in Section 3.2.

The terms "**controller**," "**data subject**," "**personal data**," "**personal data breach**," "**processor**," "**processing**" and "**supervisory authority**" have the meanings set forth in the GDPR.

2. Data Processing.

2.1. **Scope and Roles.** This DPA applies when MongoDB processes Customer Personal Data in the course of providing the Cloud Services. In this context, MongoDB is a "processor" to Customer, who may act as either a "controller" or "processor" with respect to Customer Personal Data.

2.2. **Details of the Processing.**

2.2.1. **Subject Matter.** The subject matter of the data processing under this DPA is Customer Personal Data.

2.2.2. **Duration.** The duration of the data processing under this DPA is until the expiration or termination of the MongoDB Agreement in accordance with its terms.

2.2.3. **Nature and Purpose.** The purpose of the data processing under this DPA is the provision of the Cloud Services to Customer in accordance with the MongoDB Agreement.

2.2.4. **Types of Customer Personal Data.** The types of Customer Personal Data processed under this DPA include any Customer Personal Data uploaded to the Cloud Services by Customer.

2.2.5. **Categories of Data Subjects.** The data subjects may include Customer's customers, employees, suppliers, and end users, or any other individual whose personal data Customer uploads to the Cloud Services.

2.2.6. **Processing Operations.** The objective of the processing of Customer Personal Data by MongoDB is the provision of Cloud Services to the Customer in accordance with the MongoDB Agreement.

2.3. **Compliance with Laws.** Each party will comply with all applicable Data Protection Law, including the GDPR, in relation to the processing of Customer Personal Data.

2.4. **MongoDB's Processing.** MongoDB will process Customer Personal Data only for the purposes of: (i) provisioning the Cloud Services, (ii) processing initiated by Customer in its use of the Cloud Services, and (iii) processing in accordance with your MongoDB Agreement, this DPA, and your other reasonable documented instructions that are consistent with the terms of your MongoDB Agreement. Any other processing will require prior written agreement between the parties.

2.5. **Customer Obligations.** Customer acknowledges that it controls the nature and contents of the Customer Personal Data. Customer will ensure that it has obtained all necessary and appropriate consents from and provided notices to data subjects where required by Data Protection Law to enable the lawful transfer of any Customer Personal Data to MongoDB for the duration and purposes of this DPA and the MongoDB Agreement.

3. Security.

3.1. **Confidentiality of Personnel.** MongoDB will ensure that any of our personnel and any subcontractors who have access to Customer Personal Data are under an appropriate obligation of confidentiality.

3.2. **Security Measures.** We will implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risks that are presented by the processing of Customer Personal Data. The current technical and organizational security measures are described at https://www.mongodb.com/technical-and-organizational-security-measures ("**Technical and Organizational Security Measures**").

3.3. **Optional Security Controls.** MongoDB makes available a number of security controls, features, and functionalities that Customer may elect to use, as described in the Technical and Organizational Security Measures and our Documentation. Customer is responsible for implementing those measures to ensure a level of security appropriate to the Customer Personal Data.

3.4. **Breach Notification.** We will notify you without undue delay if we become aware of a personal data breach

affecting Customer Personal Data.

4. Subprocessors.

4.1. **Authorized Subprocessors.** You acknowledge and agree that we may retain our affiliates and other third parties to further process Customer Personal data on your behalf as Subprocessors in connection with the provision of the Cloud Services. We maintain a current list of our Subprocessors at: https://www.mongodb.com/cloud/trust/compliance/subprocessors which we will update at least 30 days before the addition or replacement of any Subprocessor. You may also register to receive email notifications of any change to our list of Subprocessors.

4.2. **Subprocessor Obligations.** MongoDB will impose on each Subprocessor the same data protection obligations as are imposed on us under this DPA. We will be liable to you for the performance of the Subprocessors' obligations to the extent required by Data Protection Law.

5. Data Subject Requests.

5.1. To assist with your obligations to respond to requests from data subjects, the Cloud Services provide Customer with the ability to retrieve, correct, or delete Customer Personal Data. Customer may use these controls to assist it in connection with its obligations under the GDPR, including its obligations related to any request from a data subject to exercise their rights under Data Protection Law (each, a "**Data Subject Request**").

5.2. If a data subject contacts MongoDB with a Data Subject Request that identifies Customer, to the extent legally permitted, we will promptly notify Customer. Solely to the extent that Customer is unable to access Customer Personal Data itself, and MongoDB is legally permitted to do so, we will provide commercially reasonable assistance to Customer in responding to the Data Subject Request. To the extent legally permitted, Customer will be responsible for any costs arising from MongoDB's provision of such assistance, including any fees associated with the provision of additional functionality.

6. Cooperation. Taking into account the nature of the processing and the information available to us, at your request and cost, MongoDB will provide reasonable assistance to ensure compliance with the obligations under applicable Data Protection Law with respect to implementing appropriate security measures, personal data breach notifications, impact assessments and consultations with supervisory authorities or regulators, in each case solely related to processing of Customer Personal Data by MongoDB.

7. Government, Law Enforcement, and/or Third Party Inquiries. If MongoDB receives a request or demand to disclose Customer Personal Data to any third party, including law enforcement or a government authority ("**Third-Party Demand**"), we will attempt to redirect the Third-Party Demand to Customer. If we cannot redirect the Third-Party Demand, to the extent legally permitted, MongoDB will promptly notify Customer of the Third-Party Demand to allow Customer to seek a protective order or other appropriate remedy.

8. Customer Audit Rights.

8.1. Upon Customer's request, and subject to the confidentiality obligations set forth in your MongoDB Agreement, MongoDB will make available to Customer (or Customer's independent, third-party auditor) information regarding MongoDB's compliance with the security obligations set forth in this DPA in the form of third-party certifications and audits.

8.2. If that information is not sufficient to demonstrate our compliance with the security obligations in the DPA, you may contact MongoDB in accordance with the notice provision of your MongoDB Agreement to request an on-site audit of MongoDB's procedures relevant to the protection of personal data, but only to the extent required under applicable Data Protection Law. Customer will reimburse MongoDB for its reasonable costs associated with any such on-site audit. Before the commencement of any such on-site audit, Customer and MongoDB will mutually agree upon the scope, timing, and duration of the audit.

8.3. Customer will promptly notify MongoDB with information regarding any non-compliance discovered during the course of an audit, and MongoDB will use commercially reasonable efforts to address any confirmed non-compliance.

'

9. Data Transfers.

9.1. **Data Deployment Locations.** Customer Personal Data will only be hosted in the region(s) that Customer chooses to deploy its database clusters in its configuration of the Cloud Services (the "**Deployment Region**"). Customer is solely responsible for any transfer of Customer Personal Data caused by Customer's subsequent designation of other Deployment Regions. When required by Data Protection Law, such transfers by Customer will be governed by the transfer mechanisms described in Section 9.3 below.

9.2. **Other Processing Locations.** Use of the Cloud Services may involve transfers of Customer Personal Data outside of the EEA or the United Kingdom for other non-hosting purposes, including to provide certain features of the Cloud Services. When required by Data Protection Law, such transfers will be governed by the transfer mechanisms described in Section 9.3 below.

9.3. **Transfer Mechanism.** Where the transfer of Customer Personal Data is from the EEA or the United Kingdom to a territory which has not been recognized by the European Commission as providing an adequate level of protection for personal data on the basis of Article 45 GDPR (or in the case of transfers from the United Kingdom, by the United Kingdom Government), MongoDB agrees to process that Customer Personal Data in compliance with the Standard Contractual Clauses set out in Annex 1, which are incorporated into this DPA. MongoDB will be the "data importer" and Customer is the "data exporter" under the Standard Contractual Clauses.

10. Return or Deletion of Data. Customer may retrieve or delete all Customer Personal Data upon expiration or termination of the MongoDB Agreement. Upon termination of your MongoDB Agreement or upon your request, MongoDB will delete any Customer Personal Data not deleted by Customer, unless we are legally required to store the Customer Personal Data.

11. CCPA Obligations. MongoDB is a "service provider" as defined in the CCPA. You have provided notice to your end users that you share Customer Personal Data with your service providers. We will not retain, use, or disclose Customer Personal Data for any purpose other than providing the Cloud Services, and will not sell Customer Personal Data (as the term "sell" is described in the CCPA).

ANNEX 1

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

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

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

1. Definitions

For the purposes of the Clauses:

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

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

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data

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

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

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

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

2. Details of the transfer

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

3. Third-party beneficiary clause

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

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

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

4. Obligations of the data exporter

The data exporter agrees and warrants:

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

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

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

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

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

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

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

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

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

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

5. Obligations of the data importer

The data importer agrees and warrants:

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

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

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

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

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

(ii) any accidental or unauthorised access; and

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

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

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

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

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

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

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

6. Liability

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

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

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

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

the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

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

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

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

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

8. Cooperation with supervisory authorities

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

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

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

9. Governing law

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

10. Variation of the contract

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

11. Sub-processing

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

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer

claim for compensation referred to in paragraph 1 of Clause 3 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

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

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data-processing services

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

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

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Data exporter: The data exporter is the entity identified as the "Customer" in the Data Processing Addendum in place between data exporter and data importer, to which these Clauses are appended ("**DPA**").

Data importer: The data importer is MongoDB (as defined in the DPA), to the extent based in a country which does not ensure an adequate level of protection (within the meaning of and to the extent governed by applicable Data Protection Laws). MongoDB provides Cloud Services as described in the MongoDB Agreement (as defined in the DPA), which process Customer Personal Data upon the instruction of Customer in accordance with the terms of the MongoDB Agreement.

Description of data processing: Section 2.2 of the DPA describes the categories of data subjects, categories of data, special categories of data and processing operations.

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached): Please see the Technical and Organizational Security Measures available at https://www.mongodb.com/technical-and-organizational-security-measures.

Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and sets out the parties' interpretation of their respective obligations under specific Clauses identified below.

specific Clauses identified below.

Clause 5(f): Audit. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in Section 8 (Customer Audit Rights) of the DPA.

Clause 5(j): Disclosure of subprocessor agreements. The parties acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably can in connection with such subprocessing agreement to data exporter.

Clause 6: Liability. Any claims brought under the Clauses will be subject to any aggregate limitations on liability set out in the MongoDB Agreement.

Clause 11: Onward subprocessing. The parties acknowledge that Article 28 of the GDPR allows for the general written authorisation of a subprocessor subject to notice of and the opportunity to object to the subprocessor. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of the Standard Contractual Clauses, to engage onward subprocessors. That consent is conditional on data importer's compliance with the requirements set out in Section 4 (Subprocessors) of the DPA.