



VENDOR DATA PROCESSING ADDENDUM

NOT FOR EDITING

Effective Date: October 16, 2026

Download as PDF

This **Vendor Data Processing Addendum** (“**DPA**”) forms part of and is subject to the agreement, whether written or electronic, between Vendor (as defined below) and ClickHouse (as defined below) for the services provided by Vendor to ClickHouse (collectively, the “**Agreement**”). For the purposes of this DPA, “**ClickHouse**” means the ClickHouse entity that is party to the Agreement and “**Vendor**” means the entity identified as “**Vendor**” (or as otherwise named in the Agreement). This DPA is hereby incorporated into and made a part of the Agreement by reference.

This DPA describes the commitments of ClickHouse and Vendor (each a “**Party**” and together, the “**Parties**”) concerning the processing of Personal Data in connection with the provision of one or more services (the “**Services**”) contemplated by the Agreement. Capitalized terms not otherwise defined herein have the meaning given to them in the Agreement.

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

1.1. “**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; (ii) Canadian Privacy Laws; and (iii) 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1798.100 et seq (“**CCPA**”) as amended by the California Privacy Rights Act of 2020 (“**CPRA**”); as may be amended, superseded or replaced.

1.2. “**Canadian Privacy Laws**” means (i) the federal Personal Information Protection and Electronic Documents Act (“**PIPEDA**”), the provincial Personal Information Protection Acts in place in Alberta and British Columbia as well as An Act respecting the protection of personal information in the private sector (Québec), (ii) the E-Health (Personal Health Information Access and Protection of Privacy Act) in British Columbia, the Health Information Act in Alberta, the Personal Health Information Act in Manitoba, the Personal Health Information Protection Act, 2004 in Ontario, the Personal Health Information Privacy and Access Act in New Brunswick, the Personal Health Information Act in Newfoundland and Labrador, and the Personal Health Information Act in Nova Scotia (iii) the Canada Anti-Spam Act Legislation (“**CASL**”).

1.3. “**EEA**” means the countries that are parties to the agreement on the European Economic Area and Switzerland.

1.4. “**ClickHouse Personal Data**” means any Personal Data processed by Vendor on behalf of ClickHouse as a service provider or processor (as applicable) in connection with the Agreement, as more particularly described in [Annex I](#) of this DPA.

1.5. “**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, as amended by Directive 2009/136/EC (“**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 (“**Swiss DPA**”); and (v) in respect of the United Kingdom (“**UK**”), the Data Protection Act 2018 and the GDPR as saved into UK law by virtue of section 3 of the UK’s European Union (Withdrawal) Act 2018 (the “**UK GDPR**”) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 as they continue to have effect by virtue of section 2 of the UK’s European Union (Withdrawal) Act 2018; in each case as may be amended, superseded or replaced.

1.6. “**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.

1.7. “**Security Incident**” means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to ClickHouse Personal Data transmitted, stored or otherwise processed by Vendor and/or its Sub-processors in connection with the provision of the Services.

1.8. “**Standard Contractual Clauses**” or “**SCCs**” means the standard contractual clauses as adopted by the EU Commission by means of the Implementing Decision EU 2021/914 of June 4, 2021 found at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en.

1.9. “**Sub-processor**” means any processor engaged by Vendor 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 Vendor affiliates.

1.10. “**UK Addendum**” means the international data transfer addendum to the SCCs issued by the Information Commissioner for Parties making a transfer of personal data from the United Kingdom to any other country which is not deemed adequate under Article 46 of the UK GDPR, which is set forth in [Schedule II](#).

1.11. “**Vendor Security Addendum**” means the security standards entered into between the Parties setting forth Vendor’s technical and organization measures for the protection of Personal Data, including the minimum-security measures set forth in [Annex II](#) to the SCCs attached to this DPA.

The terms “**controller**,” “**processor**” and “**processing**” shall have the meanings given to them in the applicable European Data Protection Laws, 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**

2.1. Scope. This DPA applies to the extent that Vendor processes as a processor or service provider (as applicable) any ClickHouse Personal Data.

2.2. Role of the Parties. The Parties acknowledge and agree that ClickHouse (i) may be a processor acting on behalf of its own customers, who are controllers, with respect to the processing of ClickHouse Personal Data or (ii) is a business or the controller (as applicable) with respect to the processing of ClickHouse Personal Data, and Vendor shall process ClickHouse Personal Data only as a processor or service provider (as applicable) on behalf of ClickHouse, as further described in [Annex 1](#) of this DPA. Any processing by either Party of ClickHouse Personal Data under or in connection with the Agreement shall be performed in accordance with Applicable Data Protection Laws.

2.3. Vendor Processing of Personal Data. Vendor agrees that it shall process ClickHouse Personal Data only for the purposes described in the Agreement and in accordance with ClickHouse's documented lawful instructions. The Parties agree that the Agreement and this DPA set out ClickHouse's complete and final instructions to Vendor in relation to the processing of ClickHouse Personal Data. Vendor shall notify ClickHouse in writing, unless prohibited from doing so under Applicable Data Protection Laws, if it becomes aware or believes that any data processing instructions from ClickHouse violates Applicable Data Protection Laws. Notwithstanding anything to the contrary in the Agreement, Vendor shall not process ClickHouse Personal Data for its own internal purposes including but not limited to in an anonymized or aggregated form.

3. SUB-PROCESSING

3.1. Appointment. ClickHouse acknowledges and agrees that Vendor may engage Sub-processors to process ClickHouse Personal Data on ClickHouse's behalf. Prior to execution of the Agreement, Vendor shall provide ClickHouse with an up-to-date list of its then current Sub-processors. ClickHouse consents to Vendor's engagement of additional Sub-processors provided that:

3.1.1. Vendor shall provide at least thirty (30) days prior written notice to privacy@clickhouse.com of any change to existing Sub-processors or the engagement of any new Sub-processor (the "**Objection Period**"), and, if ClickHouse has not objected to the new Sub-processor pursuant to Section 3.2 below, Vendor shall update the list of Sub-processors authorized to process Personal Data and send such updated list to ClickHouse at privacy@clickhouse.com.

3.1.2. Vendor enters into a written agreement with each Sub-processor imposing data protection obligations no less protective of ClickHouse Personal Data as Vendor's obligations under this DPA (including the SCCs and/or other data transfer provisions) to the extent applicable to the nature of the services provided by each Sub-processor;

3.1.3. Vendor remains fully liable to ClickHouse for any breach of this DPA, the Agreement, and/or Applicable Data Protection Laws, that is caused by an act, error or omission of each Sub-processor; and

3.1.4. Upon ClickHouse's request, Vendor will provide an up-to-date list of Vendor's current Sub-processors.

3.2. Objections to Changes to Sub-processors. ClickHouse may object in writing to Vendor's appointment, or replacement of a Sub-Processor, or changes in the scope or location of the processing to existing Sub-processors, by notifying Vendor in writing within the Objection Period. ClickHouse's notification shall explain the reasonable grounds for the objection. The parties shall discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to reach resolution, Vendor will either replace or not appoint the new Sub-Processor or permit ClickHouse to suspend or terminate the affected Services (in whole or in part) in accordance with the termination provisions in the Agreement without liability to either party. Vendor will refund to ClickHouse any prepaid unused fees under the Agreement following the effective date of termination.

4. SECURITY AND AUDITS

4.1. Vendor Security Measures. Vendor shall implement and maintain appropriate technical and organizational security measures designed to protect ClickHouse Personal Data from Security Incidents and to preserve the security and confidentiality of the ClickHouse Personal Data ("**Security Measures**"). Such measures will include, at a minimum, those measures described in the Vendor Security Addendum. Vendor shall ensure that any person who is authorized by Vendor to process ClickHouse Personal Data shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.2. Security Incident Response. Upon becoming aware of a Security Incident, Vendor shall notify ClickHouse at security@clickhouse.com without undue delay and shall: (i) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by ClickHouse; and (ii) promptly take steps, necessary to contain, investigate, and remediate any Security Incident.

4.3. Security Audits. Vendor shall supply a copy of any audit reports, such as a Service Organization Control (SOC) 2 Type II or a comparable report ("**Reports**"), to ClickHouse, so that ClickHouse can verify Vendor's compliance with this DPA. In addition to the Reports, Vendor shall provide written responses (on a confidential basis) to all reasonable requests for information made by ClickHouse related to its processing of ClickHouse Personal Data, including responses to information security and audit questionnaires that are necessary to confirm Vendor's compliance with this DPA, provided that ClickHouse shall not exercise this right more than once in any twelve (12) month rolling period. In addition, ClickHouse may also conduct an audit of Vendor's data protection compliance program and compliance with this DPA if (i) the above measures are not sufficient to confirm compliance with this DPA or reveal some material issues, (ii) ClickHouse is expressly requested or required by a data protection authority to conduct such an audit, or (iii) Vendor has experienced a Security Incident.

4.4. Vendor Data Protection Measures. In addition to the Security Measures described herein, Vendor shall implement appropriate technical and organizational measures to ensure data protection for the ClickHouse Personal Data, including but not limited to: (i) measures for certification or similar assurance of data protection in processes and products; (ii) measures for ensuring data minimization; (iii) measures for ensuring data quality; (iv) measures for ensuring limited data retention; (v) measures for ensuring accountability; (vi) measures for allowing data portability where required by Applicable Data Protection Law; and (vii) measures for ensuring erasure.

5. INTERNATIONAL TRANSFERS

ClickHouse acknowledges and agrees that Vendor may transfer and process ClickHouse Personal Data to and in the United States and anywhere else in the world where Vendor, its Affiliates or its Sub-processors maintain data processing operations. Vendor shall at all times ensure such transfers are made in compliance with the requirements of Applicable Data Protection Laws and this DPA.

6. DELETION OF CLICKHOUSE PERSONAL DATA

Upon termination or expiry of the Agreement, Vendor shall delete all ClickHouse Personal Data (including copies) in its possession or control in accordance with the Agreement, save that this requirement shall not apply to the extent Vendor is required by applicable law to retain some or all of the ClickHouse Personal Data, in which case Vendor shall retain such ClickHouse Personal Data in compliance with all Applicable Data Protection Laws.

7. RIGHTS OF INDIVIDUALS AND COOPERATION

7.1. **Data Subject Requests.** To the extent that ClickHouse is unable to independently access the relevant ClickHouse Personal Data, Vendor shall, taking into account the nature of the processing, provide reasonable cooperation to assist ClickHouse to respond to any requests from individuals or applicable data protection authorities relating to the processing of ClickHouse Personal Data under the Agreement. In the event that any such request is made to Vendor directly, Vendor shall not respond to such communication directly without ClickHouse's prior authorization, unless legally compelled to do so. If Vendor is required to respond to such a request, Vendor shall promptly notify ClickHouse and provide it with a copy of the request unless legally prohibited from doing so.

7.2. **Subpoenas and Court Orders.** If a law enforcement agency sends Vendor a demand for ClickHouse Personal Data (for example, through a subpoena or court order), Vendor shall give ClickHouse reasonable notice of the demand to allow ClickHouse to seek a protective order or other appropriate remedy unless Vendor is legally prohibited from doing so, in which case Vendor shall take all reasonable steps to challenge such prohibition.

8. JURISDICTION SPECIFIC TERMS

8.1. **EEA and UK.** To the extent the ClickHouse Personal Data is subject to European Data Protection Laws, the following terms shall apply in addition to the terms in the remainder of this DPA:

8.1.1. **Sub-processor Obligations.** Vendor shall: (i) 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 (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Vendor to breach any of its obligations under this DPA.

8.1.2. **Objections to Sub-processors.** ClickHouse may object in writing to Vendor's appointment of a new Sub-processor by notifying Vendor promptly in writing within thirty (30) calendar days of receipt of Vendor notice in accordance with Section 3.1.1 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 a commercially reasonable resolution. If no such resolution can be reached, Vendor will, at its sole discretion, either not appoint Sub-processor, or permit ClickHouse 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 ClickHouse prior to suspension or termination).

8.1.3. **Data Protection Impact Assessment.** To the extent ClickHouse is required under applicable European Data Protection Law, Vendor shall provide reasonably requested information regarding Vendor processing of Personal Data under the Agreement to enable ClickHouse to carry out data protection impact assessments or prior consultations with supervisory authorities as required by law.

8.2. Restricted Transfers.

8.2.1. **Personal Data Transfers Outside of the EEA.** Any transfer by ClickHouse from the EEA and/or Switzerland to Vendor in a country outside of the EEA and/or Switzerland, where such transfer is not governed by an adequacy decision made by the European Commission or the Swiss Federal Data Protection and Information Commission, as applicable, that does not ensure an adequate level of protection under the applicable European Data Protection Law (a "**Restricted EEA and/or Switzerland Transfer**") shall be governed by and performed in accordance with the SCCs, which are incorporated by reference into this DPA and deemed executed concurrent with the execution of this DPA. [Schedule I](#) to this DPA sets forth the specific, additional and/or optional clauses for the SCCs.

8.2.2. **Personal Data Transfers Outside of the UK.** Any transfer by ClickHouse from the UK to Vendor outside of the UK, where such transfer is not governed by an adequacy decision made by the United Kingdom Secretary of State (a "**Restricted UK Transfer**" and, together with a Restricted Transfer EEA and/or Switzerland Transfer, a "**Restricted Transfer**"), shall be governed by and performed in accordance with the SCCs as modified to include the UK Addendum and their Annexes, which are (collectively) incorporated by reference into this DPA and deemed executed concurrent with the execution of this DPA. Schedule II to this DPA sets forth the specific, additional and/or optional information and clauses for the SCCs as modified to include the UK Addendum and their Annexes.

8.3. **California.** To the extent the ClickHouse Personal Data is subject to the CPRA, the Parties agree that ClickHouse is a business and that it appoints Vendor as its service provider to process ClickHouse Personal Data as permitted under the Agreement (including this DPA) and the CPRA, or for purposes otherwise agreed in writing (the "**Permitted Purposes**"). ClickHouse and Vendor agree that: (i) Vendor shall not retain, use or disclose personal information for any purpose other than the Permitted Purposes; (ii) ClickHouse Personal Data was not sold to Vendor and Vendor shall not "**sell**" personal information (as defined by the CPRA); and (iii) Vendor shall not retain, use or disclose personal information outside of the direct business relationship between ClickHouse and Vendor. Vendor certifies that it understands the restrictions set out in this Section and will comply with them.

9. MISCELLANEOUS

9.1. Except for the changes made by this DPA as applicable to the Agreement, the Agreement remains unchanged and in full force and effect; provided however that any limitations on liability and/or disclaimers of damages contained in the Agreement shall not apply to any damages arising from Vendor's breach of this DPA.

9.2. The Parties acknowledge and agree that, by executing the Agreement, ClickHouse enters into this DPA on behalf of itself and, as applicable, in the name and on behalf of its Affiliates (as defined in the underlying Agreement), thereby establishing a separate DPA between Vendor and each such Affiliate subject to the provisions of the Agreement and this Section. For the avoidance of doubt, an Affiliate is not and does not become a party to the Agreement, but is only a party to this DPA. ClickHouse shall remain responsible for coordinating all communication with Vendor under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Affiliates.

9.3. 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.

APPENDIX to the SCCs: Annexes I, II and III

ANNEX I to the SCCs

A. LIST OF PARTIES

Data exporter(s):

Name: ClickHouse, Inc.

Address: As set forth in the Agreement

Contact person's name, position and contact details: Privacy, privacy@clickhouse.com

Activities relevant to the data transferred under these Clauses: The Services described in the Agreement and its DPA Addendum

Signature and date: The Effective Date of the Agreement

Role: Controller and/or Processor

Data importer(s):

Name: Vendor

Address: As set forth in the Agreement

Contact person's name, position and contact details: Contact details as set forth in the Agreement

Activities relevant to the data transferred under these Clauses: Services described in the Agreement and its DPA Addendum

Signature and date: The Effective Date of the Agreement

Role: Processor

B. DESCRIPTION OF TRANSFER

• **Categories of data subjects whose personal data is transferred**

ClickHouse Personal Data transferred to Vendor under the Agreement may concern the following categories of data subjects: individuals whose personal data or personal information ClickHouse elects to transfer to Vendor for processing for Vendor to perform the Services as set forth in the Agreement.

• **Categories of personal data transferred**

The ClickHouse Personal Data transferred is as set forth in the Agreement and may concern the following categories of data (please specify):

- Business contact information of ClickHouse (name and business e-mail address) in all cases.
- Where ClickHouse operates as a Controller: (i) prospects, applicants, employees, agents, advisors, and subcontractors of ClickHouse; (ii) employees or contact persons of ClickHouse's prospects, customers, business partners, and vendors; and/or (iii) business contacts, marketing leads, vendors of ClickHouse.
- Where ClickHouse operates as a Processor, the categories of Personal Data are determined by ClickHouse's customer, in its sole discretion, and may include the following categories: (i) name, address, title, contact details; (ii) credit card details, account details, payment information, (iii) employer, job title, geographic location, area of responsibility; and/or (iv) IP addresses, usage data, cookie data, location data.

• **Sensitive data transferred**

The ClickHouse Personal Data transferred is as set forth in the Agreement and may concern the following special categories of data or sensitive data:

- Where ClickHouse operates as a Controller, the parties do not intend for any special category data or sensitive data to be processed under the Agreement.
- Where ClickHouse operates as a Processor, special categories of personal data or sensitive data are determined by ClickHouse's customer, in its sole discretion, and may include the following categories: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

• **Frequency of the transfer**

Data transferred on a continuous basis, or as needed, to perform the Services.

- **Nature of the processing**

ClickHouse Personal Data that ClickHouse elects to transfer for Vendor to provide the Services as set forth in the Agreement.

- **Purpose(s) of the data transfer and further processing**

The operation, support, or use of the Services as set out in the Agreement, and compliance with applicable laws.

- **The period for which the personal data will be retained**

The duration of the processing under this DPA is until the termination of the Services in accordance with the Agreement terms.

C. COMPETENT SUPERVISORY AUTHORITY

The supervisory authority of the Netherlands shall act as competent supervisory authority.

ANNEX II to the SCCs

Security Measures

The Vendor will maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data provided by the data exporter in fulfilment of the services as set forth in the Vendor Security Addendum, including the following:

1. Physical access control

Technical and organizational measures to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed. These measures include:

- Establishing security areas, restriction of access paths
- Establishing access authorizations for employees and third parties
- Access control system (ID reader, magnetic card, chip card)
- Key management, card-keys procedures
- Door locking (electric door openers etc.)
- Security staff, janitors
- Surveillance facilities, video/CCTV monitor, alarm system
- Securing decentralized data processing equipment and personal computers
- Additional measures as necessary to ensure the physical security of locations where personal data is processed

2. Virtual access control

Technical and organizational measures to prevent data processing systems from being used by unauthorized persons. These measures include:

- User identification and authentication procedures
- ID/password security procedures (special characters, minimum length, change of password)
- Automatic blocking (e.g. password or timeout)
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempt
- Creation of one master record per user, user master data procedures, per data processing environment
- Encryption of archived data media
- Endpoint protection on workstations

3. Data access control

Technical and organizational measures to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization. These measures include:

- Internal policies and procedures
- Control authorization schemes
- Differentiated access rights (profiles, roles, transactions and objects)
- Monitoring and logging of accesses
- Disciplinary action against employees who access Personal Data without authorization
- Reports of access
- Access procedure
- Change procedure
- Deletion procedure
- Encryption

4. Disclosure control

Technical and organizational measures to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed. These measures include:

- Encryption/tunneling
- Logging

- Transport security

5. Entry control

Technical and organizational measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems. These measures include:

- Logging and reporting systems
- Audit trails and documentation

6. Control of instructions

Technical and organizational measures ensuring Personal Data are processed solely in accordance with the Instructions of the Controller. These measures include:

- Unambiguous wording of the contract
- Formal commissioning (request form)
- Criteria for selecting the Processor

7. Availability control

Technical and organizational measures ensuring Personal Data are protected against accidental destruction or loss (physical/logical). These measures include:

- Backup procedures
- Mirroring of hard disks (e.g. RAID technology)
- Uninterruptible power supply (UPS)
- Remote storage of backups
- Anti-virus/firewall systems
- Disaster recovery plan

8. Separation control

Technical and organizational measures to ensure that Personal Data collected for different purposes can be processed separately. These measures include:

- Separation of databases
- “Internal client” concept / limitation of use
- Segregation of functions (production/testing)
- Procedures for storage, amendment, deletion, transmission of data for different purposes

ANNEX III to the SCCs

List of Sub-Processors

The controller has authorized the use of the Sub-processors as described in Section 3 of this DPA.

Schedule I - Transfer Mechanisms for European Data Transfers

Pursuant to Section 8.2.1 of this DPA between ClickHouse and Vendor, the SCCs are deemed incorporated into and form part of this DPA. The following specific and/or optional clauses shall apply to the SCCs as described in more detail below; any optional clauses in the SCCs not expressly selected are not included.

1. Module Two terms apply where ClickHouse is the controller of ClickHouse Personal Data and Module Three terms apply where ClickHouse is the processor of ClickHouse Personal Data.
2. The optional docking clause in Clause 7 is incorporated to this DPA.
3. For Clause 9, Option 2 (“General Authorization”) is selected and the process and time period for additional or replacement Sub-Processors shall be as set out in Section 3.1 of this DPA.
4. For Clause 17, Option 1 shall apply and the Member State for purposes of governing law shall be the Netherlands.
5. For Clause 18(b), any dispute shall be resolved by the courts of the Netherlands.
6. For Annex I.A., the “data exporter” shall be ClickHouse and the “data importer” shall be Vendor.
7. For Annex I.B., the description of the transfer is as described in Annex I to the SCCs.
8. For Annex II, the technical and organizational measures are as described in Annex II to the SCCs.
9. For Annex III, the Sub-Processors shall be as described in Annex III to the SCCs

Schedule II – Transfer Mechanisms for UK Data Transfers

Pursuant to Section 8.2.2 of this DPA between ClickHouse and Vendor, the SCCs, as supplemented by the specific and optional clauses set forth in [Schedule I](#) to this DPA (the “**EEA SCCs**”) and as modified to include the UK Addendum (the “**UK SCCs**”) are deemed incorporated into and form part of this DPA. For the avoidance of doubt, in the event of any conflict between (i) the EEA SCCs and (ii) UK SCCs, the UK SCCs shall prevail. The following information completes the UK Addendum and Annexes:

1. For Table 1 of the UK Addendum: (a) the Start Date, Parties’ Details and Key Contact are as set forth in the Order Form and Agreement and (b) the Exporter is ClickHouse and the Importer is Vendor.
2. For Table 2, the Selected SCCs, Modules and Selected Clauses are as set forth Section 8.2.1 of this DPA and [Schedule I](#) to this DPA.
3. Table 4 of the UK Addendum is modified as follows: Neither party may end the UK Addendum as set out in Section 19 of the UK Addendum; to the extent ICO issues a revised Approved Addendum under Section 18 of the UK Addendum, the parties will work in good faith to revise this DPA accordingly
4. For Annex 1A, ClickHouse and its Affiliates and Vendor are the Parties.
5. For Annex 1B, the Description of the Transfer is as set forth under Annex I.B. of this DPA.
6. For Annex II, the technical and organizational measures are as set forth in Annex II of this DPA.
7. For Annex III, the Sub-Processors shall be as described in Annex III of this DPA