

NGROK DATA PROCESSING ADDENDUM (“DPA”)

This Data Processing Agreement is between (1) the customer agreeing to the ngrok Terms of Service currently located at <https://ngrok.com/tos>, or another written agreement executed by the Parties that references this Data Processing Agreement (the “Terms”) (such customer hereinafter “Customer” or “Company”) and (2) ngrok Inc., as the provider of the Services under the Terms (hereinafter “ngrok” or “Service Provider”). Customer and ngrok together are also referred to as the “Parties” and each is also referred to as a “Party”. The DPA applies to all Processing of Customer Personal Data by Service Provider under the Agreement. Should there be a conflict between this DPA, and the Agreement, this DPA will govern.

1. Definitions. In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

- 1.1. **“Applicable Laws”** means all statutes, laws, rules, regulations, ordinances, and the like of any federal, international, city, state, provincial, or local government or governmental agency applicable to Services under the Agreement including without limitation Data Protection Laws.
- 1.2. **“Confidential Information”** is defined in the Agreement.
- 1.3. **“Customer Personal Data”** means any Personal Data provided by or made available by Customer to Service Provider or collected by Service Provider on behalf of Customer, which Service Provider Processes to perform the Services.
- 1.4. **“Data Breach”** means unauthorized acquisition of, access to, disclosure of, or use of, Customer Personal Data.
- 1.5. **“Data Protection Laws”** means Applicable Laws relating to privacy, security, or protection of Personal Data, as may be defined by such laws, including, for example and to the extent applicable, the EU General Data Protection Regulation (Regulation 2016/679) (“GDPR”); the California Consumer Protection Act (“CCPA”), regulations and official guidance adopted thereunder, and any subsequent supplements, amendments, or replacements to the same.
- 1.6. **“Data Subject”** means an identified or identifiable natural person about whom Personal Data is Processed under this Agreement or as otherwise defined (including under similar terms such as “consumer”) under Data Protection Laws.
- 1.7. **“Personal Data”** means data that that relates to an identified or identifiable natural person or as otherwise defined under Data Protection Laws.
- 1.8. **“Process, processed, or processing”** means the collection, receipt, recording, organization, structuring, alteration, use, transmission, access, sharing, provision, disclosure, distribution, copying, transfer, storage, management, retention, deletion, combination, restriction, summarizing, aggregation, correlation, inferring, derivation, analysis, adaptation, retrieval, consultation, destruction, disposal, or other handling of Personal Data.

- 1.9. **“Sell” or “selling”** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer’s Personal Data to another business or a third party for monetary or other valuable consideration.
- 1.10. **“Services”** means services provided by Service Provider under the Agreement and all schedules, order forms, and statements of work thereunder.
- 1.11. **“Share” or “sharing”** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, Personal Data to a third party for cross-context behavioural advertising (as that term is defined in the CCPA), whether or not for monetary or other valuable consideration.
- 1.12. **“Sub-processor”** means any person or entity engaged by Service Provider that Processes Customer Personal Data.
- 1.13. The terms **“Controller,” “Processor,” “Data Processor,”** and **“Business,”** shall have the same meaning as in Data Protection Laws.

2. Data Ownership/Licenses

- 2.1. **Ownership.** For purposes of this DPA, as between the parties, Customer retains all right, title, and interest in Customer Personal Data.
- 2.2. **License.** Subject to its compliance with the Agreement and DPA, Customer grants to Service Provider a worldwide, perpetual, fully paid-up right and license under all applicable intellectual property laws to make, use, copy, distribute, display, organize, create derivative works from, and otherwise Process, the Customer Personal Data, and to sublicense all the foregoing rights to Sub-processors, as necessary for the Services, rights, and obligations under the Agreement and this DPA.

3. Scope of Processing

- 3.1. **Roles of Parties.** The parties acknowledge and agree that with respect to processing of Customer Personal Data, Service Provider is a Processor and a service provider (as that term is defined in Data Protection Laws) and Customer is a Controller and Business, except that if Customer is a Processor in which case Service Provider is a Sub-processor. If Customer is a Processor of Customer Personal Data, Customer represents and warrants that Customer’s instructions and Processing of Customer Personal Data, including its appointment of Service Provider as a Sub-processor, have been authorized by the respective Controller.
- 3.2. **Details of Processing.** Exhibit 1 to this DPA (Description of Processing and Transfer Details) provides information about the subject matter and details of the Processing of Personal Data.
- 3.3. **Customer Instructions and Restrictions on Processing**
 - 3.3.1. **Instructions.** Service Provider will use, retain, and disclose Customer Personal Data solely for the specific business purpose of providing the Services and in accordance with Customer’s instructions, which are as set forth in the Agreement, DPA, and

other agreements between the parties for the Services. Service Provider will inform Customer if any of Customer's instructions infringes any Data Protection Laws.

3.3.2. **Processing by Service Provider.** Service Provider will Process Customer Personal Data in compliance with Data Protection Laws.

3.3.2.1. Service Provider will not:

- 3.3.2.1.1. Sell or Share Customer Personal Data;
- 3.3.2.1.2. use, retain, or disclose Customer Personal Data outside of its direct business relationship with the Customer;
- 3.3.2.1.3. use, retain, or disclose Customer Personal Data for any other purpose (including any other commercial purpose) other than as set forth in the Agreement and DPA, except as authorized by Customer or as required by law or by order of a court or authorized governmental agency (provided that prior notice first be given to the Customer unless such notice is prohibited by law or court order); or
- 3.3.2.1.4. combine Customer Personal Data with Personal Data that it (a) receives from or on behalf of third parties, or (b) collects from Service Provider's own interactions with Data Subjects unrelated to the Services.

3.3.2.2. Service Provider may Process Customer Personal Data:

as necessary or appropriate:

- 3.3.2.2.1. to perform its rights and obligations under the Agreement and this DPA;
- 3.3.2.2.2. to operate, manage, test, maintain and enhance the Services including as part of its business operations;
- 3.3.2.2.3. to deidentify or aggregate Customer Personal Data in a manner that prevents individual identification of the Customer, or Data Subjects;
- 3.3.2.2.4. protect the Service from a threat to the Services, Customers, Customer Personal Data, and Service Provider's systems; and
- 3.3.2.2.5. as otherwise expressly authorized by the Customer.

3.3.3. **Employees and Agents.** Service Provider will take commercially reasonable steps so that all Service Provider employees, contractors, and Sub-processors that Process Customer Personal Data are subject to written confidentiality agreements that provide substantially the same level of protection for Customer Personal Data as provided in this DPA and as required by Data Protection Laws.

3.3.4. **Unauthorized Processing.** Customer may take reasonable and appropriate steps to stop unauthorized Processing of Customer Personal Data, including without limitation, by instructing Service Provider to cease any such Processing.

3.3.5. **Deidentification.** Where Service Provider is permitted by applicable Data Protection Law or this DPA to use Customer Personal Data for its internal business purposes in a de-identified manner, Service Provider agrees to take reasonable measures designed

to ensure that the Personal Data cannot be associated with an individual (or, household, where applicable), publicly commits to maintain and use the information in de-identified form only and make no attempt to re-identify the information except where necessary to test its de-identification processes, and contractually obligates any authorized recipients to comply with these obligations.

4. Data Security

4.1. **Data Security Obligations.** Service Provider will implement and maintain commercially reasonable administrative, technical, and physical safeguards, as described in Exhibit 2.

4.2. **Data Breach.**

4.2.1. If Service Provider learns of a Data Breach affecting Customer Personal Data, Service Provider shall take reasonable, appropriate, and prompt steps to: (a) investigate, mitigate, and remedy the Data Breach; (b) notify Customer of such Data Breach without unreasonable delay consistent with timing under applicable laws; (c) furnish to Customer necessary and relevant details of the Data Breach as may be available; (d) assist Customer, as needed, in its investigation, mitigation, and remedying of the Data Breach; and (e) provide information and assist Customer, as needed, in meeting Customer's legal obligations, including any applicable obligations to notify individuals affected by the Data Breach.

4.2.2. Unless prohibited by Applicable Laws or court order, Service Provider will notify Customer if Service Provider learns of any third-party legal process relating to any Data Breach, including, but not limited to, any legal process initiated by any governmental entity.

4.2.3. Service Provider's cooperation or obligation to report or respond to Data Breaches under this DPA shall not be deemed an acknowledgment by Service Provider of any fault or liability of Service Provider with respect to a Data Breach.

4.2.4. Service Provider shall not be identified in any notifications provided publicly or to third parties (such as to government entities or Data Subjects) unless the contents of the notifications are approved by Service Provider. Service Provider agrees to cooperate in promptly reviewing any notifications and will not unreasonably withhold approval. If such reviews and approvals are expressly prohibited by Applicable Law, Customer can provide them without review and approval.

4.3. **Security Audit.** If and to the extent Service Provider processes, handles, distributes or otherwise makes available, or stores Customer Personal Data as part of the Services, then Service Provider will have facilities that process, handle and/or store such information audited annually against SOCII Type 2/SSAE 18 (or its current equivalent) standards. The summary report of any security audit will be provided to Customer upon request. Customer agrees to treat such information provided by Service Provider in response to request under this Section 4.3 as Service Provider's Confidential Information.

5. Data Protection Audits and Assistance. Upon Customer request, but no more than once per year, Service Provider will provide reasonable assistance and information to Customer regarding its Processing of Customer Personal Data to support compliance with its obligations and data protection

impact assessments, where the information sought is not provided in the Agreement or this DPA or otherwise accessible to Customer. Service Provider will also provide reasonable assistance and information to Customer to support responses to regulatory enquiries and Data Subject Rights where such means and assistance are not provided in the Agreement or this DPA or otherwise accessible to Customer through the Admin Portal. No more than once annually, Service Provider will arrange for an independent audit or assessment of policies and technological and organizational measures in support of the obligations under this DPA according to SOCII Type 2 or comparable standards and will provide a summary report of audit or assessment upon Customer request.

- 6. Notice Regarding Third Party Requests and Inquiries** Service Provider will take reasonable steps to notify Customer if Service Provider receives the following in connection with its Processing of Customer Personal Data: (i) any requests from a Data Subject, including individual opt-out requests, requests for access and/or deletion and all similar individual rights requests; or (ii) any request from a government entity or regulator provided such notice is not prohibited by law or court order.

7. Sub-processors

7.1. Approved Sub-Processors. Customer authorizes access or transfer to Service Provider's Sub-processors. At present, the Sub-processors Service Provider uses are listed in Exhibit 3 to this DPA. Service Provider will provide ten (10) calendar days' notice before utilizing a new Sub-processor by posting an update to the list at <https://trust.ngrok.com>. Customer can subscribe under trust.ngrok.com to the trust center updates and will receive notifications about any such change. Customer authorizes Service Provider to use any such Sub-processor to process Customer Personal Data unless Customer objects within ten (10) calendar days of such notification. Any such objection must be based on reasonable grounds that any such Sub-processor is unable to adequately protect the Customer Personal Data in accordance with the Agreement. If such objection is justified, Customer and Service Provider will work together to find a mutually acceptable resolution to such objection, and if unsuccessful, Customer's sole remedy is termination of the relevant Services under the terms of the Agreement.

7.2. Responsibility. Service Provider will have a written agreement in place with each Sub-processor that obligates the Sub-processor to Process Customer Personal Data in a manner that is no less protective than the obligations on Service Provider under this DPA. Where Sub-processor fails to fulfil its obligations under any sub-processing agreement or Data Protection Laws, Service Provider will remain liable to Customer for the fulfilment of its obligations under this DPA and the Agreement.

- 8. Location of Processing.** Service Provider will only Process Customer Personal Data in the countries and regions listed in Exhibit 1 and at trust.ngrok.com ("Approved Regions"), or such other countries and regions as instructed or authorized by Customer (where Customer instruction or authorization received by email or other electronic means is acceptable).

- 9. Cross-Border Data Transfers.** With regard to countries, regions, or territories with Data Protection Laws requiring a mechanism for valid export of Customer Personal Data (such countries, regions, or territories, are "Limited Transfer Region(s)" and such data is "Limited Transfer Data"), Service Provider may not transfer, export, receive, or Process such Limited Transfer Data outside of such Limited Transfer Regions unless it or its Sub-processors take measures to adequately protect such

data consistent with applicable Data Protection Laws. Such measures may include (to the extent consistent with Data Protection Laws):

- 9.1. Processing Customer Personal Data in a country, a territory, or one or more specified jurisdictions that are considered under Data Protection Laws as providing an adequate level of data protection);
- 9.2. The parties' agreement to enter into and comply with the Standard Contractual Clauses in Exhibit 4 and any successors or amendments to such clauses or such other applicable contractual terms adopted and approved under Data Protection Laws;
- 9.3. Processing in compliance with Binding Corporate Rules in accordance with Data Protection Laws;
- 9.4. Implementing any other data transfer mechanisms or certifications approved under Data Protection Laws, including, as applicable, any approved successor or replacement to the EU-US Privacy Shield framework and/or the Swiss-US Privacy Shield framework; or
- 9.5. To the extent that any substitute or additional appropriate safeguards or mechanisms under any Data Protection Laws of Limited Transfer Regions are required to transfer Customer Personal Data from a Limited Transfer Region, as applicable, to any third country, the parties agree to implement the same as soon as practicable and document such requirements for implementation in an attachment to this DPA governing the parties' Processing of Limited Transfer Data.

10. Retention and Deletion of Customer Personal Data. Upon Customer's written request, or upon termination or expiration of the Agreement, Service Provider will delete all Customer Personal Data under Service Provider's possession or control or provide Customer ability to delete such Customer Personal Data directly through tools or functionality made available by Service Provider. Service Provider will not delete to the extent that: (a) deletion is not permitted under Applicable Laws or the order of a governmental or regulatory body; (b) where Service Provider retains such data for internal record keeping, compliance with any legal obligations, and other lawfully permitted purposes; or (c) while Service Provider's then-current data retention or similar back-up system stores Customer Personal Data provided such data will remain protected in accordance with the measures described in the Agreement and this DPA.

11. General Terms

- 11.1. **Limitation of Liability.** In no event will either party: (a) be liable for any indirect, incidental, consequential, punitive, special, or exemplary damages, whether or not such damages are foreseeable or a party has been advised of the possibility thereof, arising from or relating to this DPA; and (b) have aggregate liability for damages arising from or relating to this DPA in excess of one million United States of America dollars (\$1,000,000 USD).
- 11.2. **Insurance Coverage.** During the terms of the Agreement, ngrok will maintain data security insurance sufficient to cover costs relating to Breaches described in Section 4.2 with minimum limits of one million United States of America dollars (\$1,000,000 USD).
- 11.3. **Indemnification.** Service Provider and Customer shall each indemnify, defend and hold harmless each other, and their respective directors, officers, employees and agents (and

successors, heirs and assigns) against any liability, damage, loss, fine, penalty, or expense (including reasonable attorneys' fees and costs) incurred by such indemnifying party as a result of any claim, demand, lawsuit, investigation, or regulatory enforcement proceeding arising from a breach of any obligations or restrictions of this DPA by the indemnitor ("Claim"). The indemnified party will provide the indemnitor with prompt notice of any Claim (provided that the failure to promptly notify shall only relieve indemnitor of its obligation to the extent it can demonstrate material prejudice from such failure) and at the indemnitor's expense, provide assistance reasonably necessary to defend such Claim. The indemnitor will not enter into a settlement that would result in liability to the indemnified party without the indemnified party's prior written consent, which shall not be unreasonably withheld or delayed.

- 11.4. **Termination and Survival. This DPA can be terminated as set forth in the Agreement.** The provisions of this DPA that, by their terms, require performance after the termination or expiration of this DPA, or have application to events that may occur after the termination or expiration of this DPA, will survive the termination or expiration of this DPA, including the order of precedence, and Sections 1 and 10
- 11.5. **Governing Law; Conflicts of Law; Severance.** The parties to this DPA agree to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims relating to or arising under this DPA; and this DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement (without reference to its conflict of laws requirements), unless otherwise required by Data Protection Laws. To the extent any court or governmental entity with competent jurisdiction determines that a provision of this DPA is invalid or unenforceable, the parties agree and intend that such provision should be (a) amended solely as necessary to bring it back into force in a manner consistent with the parties' manifest intent, or if that is not possible (b) severed from the DPA in a manner to give maximum legal force and effect to the remaining provisions

Service Provider:

ngrok
548 Market St
PMB 26741
San Francisco, CA 94104-5401 USA

Service Provider Contact:

support@ngrok.com

EXHIBIT 1
DETAILS OF PROCESSING OF CUSTOMER PERSONAL DATA

This Exhibit 1 supplements the Agreement and DPA, and together, provide details about Customer Personal Data processing by Service Provider.

Describe the Customer Business Purpose, including the nature and purpose of the Processing of Customer Personal Data. "Customer Business Purpose" is the purpose for which Customer is authorizing Service Provider to Process Customer Personal Data in connection with providing the Services to Customer, as further described in the Agreement and Exhibit 1 to this DPA.

Providing Services as agreed between ngrok and the Customer

The types of Customer Personal Data to be Processed

Contact information

Configuration data (such as domain names, IP addresses, and potentially authentication keys)

Communications content data (potentially any information that is personal data that is processed via ngrok's Services)

The Types of Sensitive Customer Personal Data to be Processed

None

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

Customer employees

Customer's consumer customers

The frequency of the transfer of Customer Personal Data from Customer to Service Provider

Continuous

Duration of the Processing of Customer Personal Data

Subject to the terms of this DPA and the Agreement and as determined by Customer, but generally duration of the Customer's Agreement with ngrok

Location of Processing of Customer Personal Data by Service Provider

See also Sub-processor and location list at <https://trust.ngrok.com>

The obligations and rights of Customer

The obligations and rights of Customer are set out in the Agreement and this DPA

EXHIBIT 2

INFORMATION SECURITY MEASURES

Service Provider's personnel will not process Customer Personal Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer Personal Data and this obligation continues even after their engagement ends.

The technical and organizational measures implemented by Service Provider to provide an appropriate level of security include:

Measures of pseudonymization and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

Measures for user identification and authorization

Measures for the protection of data during transmission

Measures for the protection of data during storage – all data is encrypted at rest.

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging, including keeping audit logs.

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure

Additional details about ngrok's information security measures can be found at <https://trust.ngrok.com/>.

EXHIBIT 3
SUB-PROCESSORS

The Sub-processors authorized to Process Customer Personal Data are listed at <https://trust.ngrok.com/>.

EXHIBIT 4
STANDARD CONTRACTUAL CLAUSES

The parties agree that Limited Transfer Data transferred between and among the parties shall be subject to the Standard Contractual Clauses to the extent applicable. Without limitation: (i) transfers of Limited Transfer Data from the European Economic Area (“EEA”) or Switzerland (or Limited Transfer Data subject to Data Protection Laws in the EEA or Switzerland) to Third Countries are subject to the Standard Contractual Clauses in this Exhibit 4; (ii) transfers of Limited Transfer Data from the United Kingdom (“UK”) (or Limited Transfer Data subject to Data Protection Laws in the UK) to Third Countries are subject to the Standard Contractual Clauses in this Exhibit 4 as supplemented by the UK Transfer Addendum in this Exhibit 4.

(A) The parties acknowledge the importance of the protection of Personal Data and the legal restrictions on international transfers of Personal Data.

(B) Accordingly, the parties agree to abide by the GDPR, UK GDPR and Data Protection Act 2018, Swiss Federal Data Protection Act, and other Data Protection Laws of Limited Transfer Regions recognizing the Standard Contractual Clauses or similar principles, as applicable, and enter into these Standard Contractual Clauses to ensure that Customer Personal Data transfers outside any Limited Transfer Regions to any third country other than a country, region, or territory that the relevant data authority has not determined to offer an adequate level of data protection are lawful and subject to adequate data protections. To the extent processing of Customer Personal Data by the data importer is subject to Article 3(2) of the GDPR, this Exhibit 4 shall not apply.

1. CLARIFICATION OF DEFINITIONS & TERMS

(A) The terms “data controller” or “controller,” “data exporter,” “data importer,” “data processor” and “Personal Data” shall have the meaning under the GDPR, UK GDPR and Data Protection Act 2018, Swiss Federal Data Protection Act, or applicable Data Protection Laws of Limited Transfer Regions as applicable.

(B) For Limited Transfer Regions outside the EU, references to the General Data Protection Regulation will be replaced by applicable Data Protection Laws of the respective Limited Transfer Regions and for Clause 13 references to EU Member State shall be replaced with the applicable Limited Transfer Region. If Switzerland is the Limited Transfer Region: references to “Regulation (EU) 2016/679” and any articles therefrom shall be interpreted to include references to the Swiss DPA; and references to “EU”, “Union” and “Member State” shall be interpreted to include references to “Switzerland”.

(C) Section 1 Clause 1 (a) of the Standard Contractual Clauses (Definition of Data Importer): The “data importer” means Service Provider.

(D) Section 1 Clause 1 (a) of the Standard Contractual Clauses (Definition of Data Exporter): The “data exporter” means Customer.

(E) With respect to objections to subprocessors under Section 1 Clause 9, the parties will work together to find a mutually acceptable resolution to such objection, and if unsuccessful, Customer’s sole remedy is termination of the relevant Services under the terms of the Agreement

2. APPLICABLE MODULES

With respect to Processing of Customer Personal Data, Customer is a Data Exporter and Controller, and Service Provider is a Data Importer and Processor - Module Two shall apply. The following modules shall not apply, and language specific to those modules shall not be treated as part of this Agreement: Module One, Module Three, and Module Four.

3. AMENDMENTS OR UPDATES

The parties agree that to the extent that any additional appropriate safeguards under Data Protection Laws of Limited Transfer Regions recognizing the Standard Contractual Clauses or similar principles are required to export data to any third country, or to the extent that the Standard Contractual Clauses are substituted or replaced or not recognized under any such law, the parties agree to either promptly implement the same or agree to use another acceptable method for transfer of such data and promptly amend this Exhibit 4 as necessary to comply with such requirements.

4. CONFLICTS

If the terms of the Agreement or the DPA conflict with the Standard Contractual Clauses, the terms of the Standard Contractual Clauses will prevail.

5. EU SCC and UK Transfer Addendum Information.

SCC Clause	GDPR	Swiss DPA	UK Data Protection Law
Module in Operation Module Two (Controller to Processor)			
Clause 7- Docking Clause	Optional language in Cause 7 shall not apply.		
Clause 9(a)- Use of Sub-processors	Module Two - OPTION 2 shall apply: GENERAL WRITTEN AUTHORISATION: 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 at least 10 days in advance, 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.		
Clause 11 - Redress	Optional language in Clause 11 shall not apply.		
Clause 17- Governing Law	Option 2 (for Module Two) shall apply: The Parties agree that this shall be the law of the Member State where the Customer is established. Customer will identify such Member State to ngrok upon request.	These Clauses shall be governed by the law of Switzerland, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Switzerland.	These Clauses shall be governed by the law of the United Kingdom, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of England and Wales.

Clause 18 – Choice of Forum and Jurisdiction	The parties agree that those shall be the courts of Ireland.	The parties agree that those shall be the competent courts of Switzerland.	The parties agree that those shall be the competent courts of England and Wales.
Appendix, Annex I.A- List of Parties	The name, address, and contact person's name, position, and contact details, and each party's role in Processing Personal Data are as set forth in the DPA and Exhibit 1 to the DPA to which this Exhibit 4 is attached.		
Annex I>B – Description of Transfer	This information can be found in Exhibit 1 to the DPA to which this Exhibit 4 is attached. To the extent applicable, the descriptions of safeguards applied to the special categories of Personal Data can be found Exhibit 2 to the DPA to which this Exhibit 4 is attached.		
Clause 13 and Annex I>C – Competent Supervisory Authority	The parties agree that Customer will communicate the relevant supervisory authority to ngrok upon request.	Identify the competent supervisory authority/ies in accordance with Clause 13: FDPIC	Identify the competent supervisory authority/ies in accordance with Clause 13: UK Information Commissioner
Annex II – Technical and Organizational Measures	The description of technical and organization measures designed to ensure the security of Personal Data is in Exhibit 2 to the DPA to which this Exhibit 4 is attached.		
Annex II – Technical and Organizational Measures – Subprocessors	The description of technical and organization measures designed to ensure the security of Personal Data are described more fully Exhibits 2-3 to the DPA to which this Exhibit 4 is attached.		
Annex III – List of Subprocessors	As described in Exhibit 3 to the DPA to which this Exhibit 4 is attached.		
Ending the UK Transfer Addendum when the Approved Addendum changes	N/A		Which Parties may end this Addendum as set out in Section 19: <input checked="" type="checkbox"/> Importer <input checked="" type="checkbox"/> Exporter <input type="checkbox"/> neither Party

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)¹ 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.

¹ Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

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:
 - (ii) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - (iii) 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);
 - (iv) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
 - (v) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
 - (vi) Clause 13;
 - (vii) Clause 15.1(c), (d) and (e);
 - (viii) Clause 16(e);
 - (ix) 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

Docking clause

Intentionally omitted

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 anonymisation² 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.

² This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

- (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 Union³ (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

³ The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

- (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 Union⁴ (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

⁴ The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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 exporter⁵.

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

⁵ See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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 Union⁶ (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

⁶ The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

- (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.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

- (a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- (b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- (c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- (d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify

to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

- (a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and 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 of the personal data⁷, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and 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 data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- (c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

- (a) **GENERAL WRITTEN AUTHORISATION** 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 at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the

⁷ This includes whether the transfer and further processing 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.

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.⁸ 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) **GENERAL WRITTEN AUTHORISATION** 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 at least [*Specify time period*] in advance, 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

⁸ This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

⁹ This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.¹⁰ 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

¹⁰ That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

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 lay 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.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

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

- (g) 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.
- (h) 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.
- (i) 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.
- (j) 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.
- (k) 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

- (l) 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.
- (m) 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.
- (n) 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.

- (o) 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.
- (p) 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.
- (q) 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.
- (r) 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 safeguards¹¹;

¹¹ As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical

- (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.

experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

- (f) 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).
- (g) 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.]
- (h) 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

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 Ireland.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

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 Ireland.
- (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.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of _____ (*specify country*).

APPENDIX

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s):

Name: Company name is as provided below the signature line of this DPA.

Address: Company address is as provided below the signature line of this DPA.

Contact person's name, position and contact details: Details provided below the signature line of this DPA.

Activities relevant to the data transferred under these Clauses: As described in Exhibit 1 to this DPA.

Signature and date: Provided in the signature line of this DPA.

Role (controller/processor): Role of Company as specified in Section 3.1 of this DPA.

Data importer(s):

Name: ngrok.

Address: ngrok address is as provided below the signature line of this DPA.

Contact person's name, position and contact details: Details provided below the signature line of this DPA.

Activities relevant to the data transferred under these Clauses: As described in Exhibit 1 to this DPA.

Signature and date: Provided in the signature line of this DPA.

Role (controller/processor): Role of Service Provider as specified in Section 3.1 of this DPA.

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred

As described in Exhibit 1 to this DPA.

Categories of personal data transferred

As described in Exhibit 1 to this DPA.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As described in Exhibits 1-2 to this DPA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As described in Exhibit 1 to this DPA.

Nature of the processing

As described in Exhibit 1 to this DPA.

Purpose(s) of the data transfer and further processing

As described in Exhibit 1 to this DPA.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As described in Exhibit 1 to this DPA.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described in Exhibit 3 to this DPA.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

.....

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES - TECHNICAL AND ORGANISATIONAL MEASURES

INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

As described in Exhibit 2 to this DPA.

ANNEX III TO THE STANDARD CONTRACTUAL CLAUSES – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

As described in Exhibit 3 to this DPA.

EXHIBIT 4 CONTINUED

UK TRANSFER ADDENDUM TO STANDARD CONTRACTUAL CLAUSES



Information Commissioner's Office

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date		
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	<p>Full legal name: Customer, as provided in the DPA to which this Exhibit 4 is attached.</p> <p>Trading name (if different): <input type="text"/></p> <p>Main address (if a company registered address): Customer address, as provided in the DPA to which this Exhibit 4 is attached</p> <p>Official registration number (if any) (company number or similar identifier): <input type="text"/></p>	<p>Full legal name: Service Provider, as provided in the DPA to which this Exhibit 4 is attached</p> <p>Trading name (if different): <input type="text"/></p> <p>Main address (if a company registered address): Service Provider address, as provided in the DPA to which this Exhibit 4 is attached</p> <p>Official registration number (if any) (company number or similar identifier): <input type="text"/></p>

Key Contact	<p>Full Name (optional): Customer signatory, as provided in the DPA to which this Exhibit 4 is attached</p> <p>Job Title: Customer signatory, as provided in the DPA to which this Exhibit 4 is attached</p> <p>Contact details including email: Customer signatory, as provided in the DPA to which this Exhibit 4 is attached</p>	<p>Full Name (optional): Service Provider signatory, as provided in the DPA to which this Exhibit 4 is attached</p> <p>Job Title: Service Provider signatory, as provided in the DPA to which this Exhibit 4 is attached</p> <p>Contact details including email: Service Provider signatory, as provided in the DPA to which this Exhibit 4 is attached</p>
Signature (if required for the purposes of Section 2)	Customer signature, as provided in the DPA to which this Exhibit 4 is attached	Service Provider signature, as provided in the DPA to which this Exhibit 4 is attached

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	<p><input checked="" type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:</p> <p>Date: Effective Date of the DPA to which this Exhibit 4 is attached.</p> <p>Reference (if any): Standard Contractual Clauses as contained in this Exhibit 4 to the DPA.</p> <p>Other identifier (if any): </p>
-------------------------	--

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	N/A. As described in the version of Standard Contractual Clauses contained in this Exhibit 4 to the DPA.					
2						

3	
4	

Table 3: Appendix Information

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: as provided in the DPA to which this Exhibit 4 is attached.

Annex 1B: Description of Transfer: as provided in Exhibit 1 to the DPA to which this Exhibit 4 is attached

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: as provided in Exhibit 2 to the DPA to which this Exhibit 4 is attached

Annex III: List of Sub processors (Modules 2 and 3 only): as provided in Exhibit 3 to the DPA to which this Exhibit 4 is attached

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: Exporter and/or Importer
---	---

Part 2: Mandatory Clauses

Entering into this Addendum

- Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
- Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out

in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

4.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
 - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

- b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
 - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
- 13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
- 14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
- 15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
 - a. References to the “Clauses” means this Addendum, incorporating the Addendum EU SCCs;
 - b. In Clause 2, delete the words:

“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”;
 - c. Clause 6 (Description of the transfer(s)) is replaced with:

“The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter’s processing when making that transfer.”;
 - d. Clause 8.7(i) of Module 1 is replaced with:

“it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer”;
 - e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”
 - f. References to “Regulation (EU) 2016/679”, “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)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;
 - g. References to Regulation (EU) 2018/1725 are removed;

- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;
- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;
- j. Clause 13(a) and Part C of Annex I are not used;
- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;
- l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;
- m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;
- n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and
- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

- 16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
- 17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
- 18. From time to time, the ICO may issue a revised Approved Addendum which:
 - a. **makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or**
 - b. **reflects changes to UK Data Protection Laws;**

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum

including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 “Ending the Addendum when the Approved Addendum changes”, will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
- a. its direct costs of performing its obligations under the Addendum; and/or
 - b. its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.
--------------------------	---