Data processing agreement

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**") and (2) ngrok Inc., as the provider of the Services under the Terms (hereinafter "**ngrok**"). Customer and ngrok together are also referred to as the "**Parties**" and each is also referred to as a "**Party**".

1. General provisions

1.1 Customer is the controller according to the European General Data Protection Regulation ("**GDPR**"). ngrok is processing personal data on behalf of the Customer, thus a processor according to the GDPR, or a sub-processor where Customer is itself a processor to another controller.

1.2 ngrok processes personal data in order to fulfil its obligations under the Terms on behalf of Customer in accordance with Art. 4(2) and Art. 28 of the GDPR solely based on this Data Processing Agreement ("**DPA**") and Customer's instructions.

1.3 The subject matter of the processing results from the Terms.

1.4 Beginning and duration of the processing depend on the beginning and duration of the Terms.

1.5 Unless stipulated otherwise in the DPA, the terms used herein shall have the meaning ascribed to them in the Terms.

2. Nature and purpose of the processing, type of personal data and categories of data subjects

2.1 Under this DPA, ngrok will process Customer's communications content data (potentially any information that is personal data that is processed via nrogk's services (the "**Services**") as agreed (solely subject to Customer's discretion); contact information; configuration data (such as domain names, as far as these are personal data, IP addresses, and potentially authentication keys)) and any content of Customer's customers (i.e their respective data subjects) or other data subjects that are somehow involved in the processing of Customer when using the Services (solely subject to Customer's discretion) as agreed between ngrok and the Customer. Further details of the processing activities undertaken by ngrok on behalf of Customer result from the Terms.

2.2 The purpose of the processing is to provide the Services as agreed between ngrok and the Customer and subject to the Terms.

2.3 The processing activities concern personal data of Customer's customers.

3. Customer's rights and obligations; instruction rights

3.1 It is the sole responsibility of Customer to assess the legitimacy of the processing. If not set out differently, this includes the handling of data subjects rights. ngrok will forward to Customer any data subject's rights request clearly addressed to Customer.

3.2 Any orders, partial orders and instructions given by Customer in general shall be in writing or in a documented electronic form.

3.3 Changes of the subject-matter of the processing or of procedures shall be coordinated between Customer and ngrok and established in writing or in a documented electronic form.

3.4 ngrok ensures that Customer or a third party instructed by Customer can verify the implementation and adequacy of the technical and organizational measures by ngrok before and during the processing (including on-site inspections). Upon request, ngrok will provide Customer with a written report (from a third party) that ngrok fulfills all necessary requirements regarding the technical and organizational measures. Where Customer does not object to the findings, such report fulfills the audit obligations under the GDPR.

4. ngrok's obligations

4.1 ngrok processes personal data solely within the scope of this DPA and upon instructions of Customer, unless required to do so by European Union or member state law to which ngrok is subject. In such a case, ngrok shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

4.2 ngrok shall take appropriate technical and organizational measures for the processing of the personal data (Art. 32 GDPR).

4.3 ngrok shall contribute to and support Customer to the best of its ability when it comes to fulfilling the rights of data subjects according to Art. 12 to 22 of the GDPR by Customer, to

the creation of records of processing activities (Art. 30 of the GDPR) and to a necessary data protection impact assessment (Art. 35 of the GDPR). ngrok shall immediately forward the required information to Customer. Customer will reasonably reimburse ngrok for any such contribution or support.

4.4 ngrok shall immediately bring to Customer's attention if, in ngrok's opinion, an instruction issued by Customer violates statutory provisions.

4.5 ngrok shall correct, delete or restrict the processing of personal data upon Customer's instruction, unless statutory provisions or legitimate interests of ngrok require ngrok not to do so. ngrok shall be entitled to provide information concerning personal data under this DPA to third parties or the data subject only upon Customer's prior instruction or consent, unless such provision is part of using the Services.

4.6 ngrok confirms to be aware of the applicable data protection provisions of the GDPR. ngrok agrees to be bound by confidentiality with regard to processing Customer's personal data under this DPA during and after the contractual relationship between the Parties.

4.7 ngrok shall ensure that each person having access to Customer's personal data is bound to data secrecy and informs them of all relevant data protection obligations according to this DPA as well as the obligation to act on Customer's instructions.

5. ngrok's notification obligations

5.1 ngrok shall notify Customer of any malfunctions, infringements by ngrok or the persons employed by ngrok of data protection provisions or the stipulations made in the DPA or an instruction as well as any suspected data protection infringements or irregularities in the processing of personal data without undue delay as soon as they become known to ngrok.

5.2 ngrok shall provide adequate support to Customer regarding Customer's obligations according to Art. 33 and 34 of the GDPR.

6. Sub-processors

6.1 ngrok only may use sub-processors with Customer's prior consent. Customer agrees to the sub-processors as listed in **Annex 1**. If Customer has a reasonable basis to object to ngrok's use of a new sub-processor, Customer shall notify ngrok promptly in writing within seven (7) days after receipt of ngrok's notice regarding such new sub-processor. In the

event Customer objects to a new sub-processor(s) on a reasonable basis, ngrok will use reasonable efforts to work in good faith with Customer to find an acceptable, reasonable, alternate solution. If the Parties are not able to agree to an alternate solution within a reasonable time (no more than 30 days), Customer may terminate the Terms in respect only to the specific service which cannot be provided by ngrok without the use of the objected-to new sub-processor, by providing written notice to ngrok.

6.2 ngrok will contractually ensure that ngrok's obligations agreed on in this DPA also apply to all sub-processors.

6.3 ngrok shall remain responsible to Customer for sub-processor's obligations.

7. Transfer of personal data to countries outside the EU

7.1 The Parties conclude the standard contractual clauses in **Annex 2**.

7.2 Where ngrok transfers personal data to another controller or processor outside of the EU (as far as allowed under the DPA), ngrok will fulfil all necessary requirements under the GDPR.

8. Technical and organizational measures according to Art. 32 of the GDPR

A level of protection adequate to the risk to the rights and freedoms of the data subjects shall be ensured with regard to the processing under this DPA.

9. Obligations of ngrok after termination of the processing

After the termination of the procession under this DPA, ngrok shall, at Customer´s choice, hand over, delete in accordance with data protections regulations, or have deleted accordingly, all data, documents and processing or usage results in connection with the processing being in its possession.

10. Final provisions

If this DPA contradicts other agreements concluded between the Parties, the provisions of this DPA shall take precedence.

Annex 1

Amazon Web Services, Segment, HubSpot

Annex 2

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to

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

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

Clause 3

Third-party beneficiaries

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

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

(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(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

(Intentionally left blank)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the

duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (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 benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least one (1) week 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.

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

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

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

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

Clause 10

Data subject rights

(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.

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.

(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

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

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

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its subprocessor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the

data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

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

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

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

Clause 13

Supervision

(a) [WHERE CUSTOMER IS ESTABLISHED IN THE EU:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679, as indicated in Annex I.C, shall act as competent supervisory authority as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[WHERE CUSTOMER IS ESTABLISHED OUTSIDE THE EU AND HAS DESIGNATED A REPRESENTATIVE ACCORDING TO ART. 27(1) OF THE GDPR:] 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.

[CUSTOMER IS ESTABLISHED OUTSIDE THE EU AND HAS NOT DESIGNATED A REPRESENTATIVE ACCORDING TO ART. 27(2) OF THE GDPR:] 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

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

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

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

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

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

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

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

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

(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. 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 the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

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.

(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.).

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

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the

competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

In these cases, it shall inform the competent supervisory authority 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) 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. 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

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 Germany [alternatively: where the Customer is located within the EU, otherwise Germany].

Clause 18

Choice of forum and jurisdiction

(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 Germany [alternatively: where the Customer is located within the EU, otherwise Germany].

(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.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s): Customer, agreeing to the Terms.

Data importer(s): ngrok, as the provider of the Services.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Customer's customers (i.e their respective data subjects) or other data subjects that are somehow involved in the processing of Customer when using the Services (solely subject to Customer's discretion) as agreed between ngrok and the Customer

Categories of personal data transferred

Potentially any information that is personal data and that is processed via the Services as agreed (solely subject to Customer's discretion), including contact information, configuration data (such as domain names, as far as these are personal data, IP addresses, and potentially authentication keys)) and any content of Customer's customers (i.e their respective data subjects) or other data subjects that are somehow involved in the processing of Customer when using the Services (solely subject to Customer's discretion) as agreed between ngrok and the Customer.

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 per the Terms, sensitive data is not part of the Services made available by ngrok.

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

Continuous basis.

Nature of the processing

Providing the Services described in the Terms to Customer.

Purpose(s) of the data transfer and further processing

The purpose of the processing is to provide the Services as agreed between ngrok and the Customer and subject to the Terms

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

Duration of the agreement between ngrok and Customer.

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

Providing technical help in providing the Services of ngrok for the duration of the agreement.

C.COMPETENT SUPERVISORY AUTHORITY

The supervisory authority competent for the Customer.

ANNEX II – TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Implemented technical and **organizational measures**

Processor has implemented the following technical and organizational measures to protect personal data:

1.	Does a security concept pursuant to Art. 32 GDPR exist?	✓ yes ☐ no
2.	Have measures of physical access control been implemented that prevent unauthorized persons from physically accessing systems, data processing facilities or operations?	✓ yes ☐ no *Measures:* ✓ access control systems, readers (magnetic/chip card) ✓ Key administration/documentation of key distribution ✓ Securing doors (electric opening of doors, combination locks, etc.) ✓ Employee or entitlement cards ✓ Supervision of external persons inside the building ✓ Registration or escorting of visitors
3.	Have measures of technical access control been implemented that prevent unauthorized persons from accessing data processing systems?	✓ yes ☐ no *Measures:* ✓ Personal and individual login for the use of systems or company networks and, if necessary, further access identification ✓ Password assignment (definition of password requirements regarding complexity and update intervals) ✓ Separate system login for certain applications ✓ Automated closing of programs after a defined period without user activity (equally, password-protected screen saver or automated setup of work breaks) ✓ Security training and ensuring attentiveness of employee (including training on phishing and social engineering)
4.	Have measures of data access control been implemented that ensure access of entitled persons only and their limited access to the data included in their access rights?	✓ yes ☐ no *Measures:* ✓ Administration of access (role concept) ✓ Differentiated entitlements ✓ Profiles ✓ Roles ✓ Documentation of entitlements ✓ Routine of approval ✓ Audits / monitoring (e.g. of ISO certification, SOX compliance)

		✓ Encryption of CD/DVD-ROM, external hard drives and/or laptops (e.g. via OS, True Crypt, Safe Guard Easy, WinZip, PGP) ✓ Distribution of obligations
5.	Have measures of data transport control been implemented that secure confidentiality and integrity of personal data when transferred as well as of data carrier transfers?	✓ yes ☐ no *Measures:* ✓ Encryption of CD/DVD-ROM, external hard drives and/or laptops (e.g. via OS, True Crypt, Safe Guard Easy, WinZip, PGP) ✓ Encrypted data transfer connections (VPN = Virtual Private Network) ✓ SSL encryption of internet connection ✓ Rules on destruction of data carriers etc.
6.	Have measures to prevent unauthorized reading, copying, modification, or deletion of data carriers been implemented?	✓ *yes* ☐ *no* *Measures:* ✓ Encryption of CD/DVD-ROM, external hard drives and/or laptops (e.g. via OS, True Crypt, Safe Guard Easy, WinZip, PGP) ✓ Securing transport of data carriers ✓ Policy on deletion/destruction/erasure of data carriers etc.
7.	Have measures to prevent unauthorized input of data as well as unauthorized access, modification, and deletion of stored personal data been implemented?	✓ *yes* ☐ *no* *Measures:* ✓ Personal and individual login for the use of systems or company networks ✓ Password assignment (definition of password requirements regarding complexity and update intervals) ✓ Profiles ✓ Roles ✓ Security training and ensuring attentiveness of employees (including training on phishing and social engineering)
8.	Have measures to control data input that allows determining who has accessed, modified, deleted, or transferred personal data been	✓ yes ☐ no *Measures:* ✓ Access authorization ✓ Registration within the system

	implemented and in which way?	
9.	Access to personal data and documents	Is every login, input, modification, deletion, and transfer registered? (Accesses for reading must also be observed, if necessary.) ☐ yes ✓ no
10.	Have measures in enter control been implemented to ensure that the processing of personal data is conducted strictly according to Controller's directives?	✓ yes ☐ no *Measures:* ✓ Briefing of all employees authorized of access ✓ Regular additional briefings ✓ Pledging employees to confidentiality according to Art. 28(3)(2)(b) GDPR ✓ Regular data protection controls by the internal data protection officer ✓ Naming of contact persons and responsible project managers for the specific assignment ✓ Internal guidelines for handling data-sensitive situations
11.	Have measures of availability control been implemented that protect against incidental destruction or loss of personal data?	✓ yes ☐ no *Measures:* ✓ Backup procedure ✓ Storage on hard drives "mirroring" ✓ Ensuring uninterrupted power supply ✓ Retention possibility for backups (secure, separate areas, etc.) ✓ Virus protection / firewall ✓ Usage of safe and resilient servers ✓ Server virtualization ✓ Appropriate ways of archiving ✓ Contingency plan ✓ Emergency exercises ✓ Emergency plans ✓ Error and restoring plans, etc.
12.	Have measures for compliance with the requirement of data separation been implemented, so that personal data collected	✓ yes ☐ no *Measures:* ✓ Separated systems ✓ Separated data bases

	for different purposes is processed separately?	✓ Access authorization (e.g., for responsible employees and certain applications only) ✓ Separation by means of logical access regulation
13.	Have measures been implemented that ensure recoverability of systems in the event of a malfunction?	✓ *yes* ☐ *no* *Measures:* ✓ Backups ✓ Storage on hard disks “mirroring” ✓ Retention possibility for backups (secure, separate areas, etc.)
14.	Have measures that ensure all functions of the systems used are available and any malfunctions that occur are reported been implemented?	✓ *yes* ☐ *no* *Measures:* ✓ Virus protection / firewall ✓ Usage of safe and resilient servers ✓ Plans for notification of malfunctions that occur ✓ Automated processes for displaying malfunctions
15.	Have measures to prevent the damage of stored personal data resulting from malfunctions of the system been implemented?	✓ *yes* ☐ *no* *Measures:* ✓ Backups ✓ Storage on hard disks “mirroring” ✓ Retention possibility for backups (secure, separate areas, etc.)

ANNEX III – LIST OF SUB-PROCESSORS

See Annex 1 above.