Data Processing Addendum

This Data Processing Addendum (“Addendum”) is executed by and between “Processor” Epik LLC and its Affiliates (collectively “Epik”) and you (“Controller”, “Customer”) annexes into and supplements our General Terms of Service, Privacy Policy, and any and all other agreements governing our Services (collectively, the “Terms of Service”). Unless otherwise defined in this Addendum, references to "we", "us" and "our(s)" refer to Epik and all capitalized terms not defined in this Addendum will have the meanings given to them in the Terms of Service.

1. Definitions

“Affiliates” means any entity which is controlled by, controls, or is in common control with Epik LLC.

“Covered Services” means hosted services we offer you that could involve our Processing of Personal Data.

“Customer Data” means the Personal Data of any Data Subject Processed by us within the Epik Network on behalf of Customer pursuant to or in connection with the Terms of Service.

“Data Controller” means the you, the Customer, as the entity which determines the purposes and means of the Processing of Personal Data.

“Data Processor” means us, Epik, as the entity which Processes Personal Data on behalf of the Data Controller.

“Data Protection Laws” means the GDPR (as defined below), together with any national implementing laws in any Member State of the European Union or the United Kingdom or, to the extent applicable, in any other country, in each case as amended, repealed, consolidated, or replaced from time to time.

“Data Subject” means the individual to whom Personal Data relates.

“EEA” means the European Economic Area.

“GDPR” means the General Data Protection Regulation (EU) in regards to the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

“Epik Network” means our data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within our control and are used to provide the Covered Services.

“Personal Data” means any information relating to an identified or identifiable person.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. “Process”, “processes” and “processed” will be interpreted accordingly. Detail of Processing are set forth in Annex 1.

“Security Incident” means either (a) a breach of security of our Security Standards leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Data; or (b) any unauthorized access to our equipment or facilities, where in either case such access results in destruction, loss, unauthorized disclosure, or alteration of Customer Data.

“Security Standards” means the security standards attached to this Addendum as Annex 2.

“Sensitive Data” means (a) social security number, passport number, driver’s license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a card number), financial information, banking account numbers, or passwords; (c) employment, financial, genetic, biometric, or health information; (d) racial, ethnic, political, or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords, mother’s maiden name, or date of birth; (f) criminal history; or (g) any other information or combinations of information that falls within the definition of “special categories of data” under GDPR or any other applicable law or regulation relating to privacy and data protection.

“Standard Contractual Clauses” or “SCCs” means the standard data protection clauses for the transfer of personal data from a controller to a processor established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR.

“Sub-processor” means any Data Processor engaged by Processor to Process data on behalf of Data Controller.

“UK Standard Contractual Clauses” or “UK SCCs” means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the UK GDPR.

2. Data Processing

a. Scope and Roles. This Addendum applies when Customer Data is processed by us. In this context, we will act as the Data Processor on behalf of the Customer as the Data Controller with respect to Customer Data.

b. Details of Data Processing. The subject matter of processing of Customer Data by us is the performance of the Covered Services pursuant to the Terms of Service and product-specific agreements. We shall only Process Customer Data on behalf of and in accordance with Customer’s documented instructions for the following purposes: (i) Processing in accordance with the Terms of Service or applicable product-specific agreement; (ii) Processing initiated by end users in their use of the Covered Services; (iii) Processing to comply with other documented, reasonable instructions provided by Customers where such instructions are consistent with the terms of this Addendum. We shall not be required to comply with or observe Customer’s instructions if such instructions would violate the Data Protection Laws. The duration of the Processing, the nature and purpose of the Processing, the types of personal data and categories of Data Subjects Processed under this Addendum are further specified in Annex 1 (‘Details of the Processing’) to this Addendum.

c. For the avoidance of doubt, Customer’s instructions for the Processing of Personal Data shall comply with all applicable data privacy laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

3. Confidentiality of Customer Data

We do not not voluntarily provide governments with access to any data about users for surveillance purposes, and we will not disclose Customer Data to any government or any other third party, except as necessary to comply with the law or a valid and binding order of a law enforcement agency (such as a subpoena or court order). All legal process is carefully reviewed to ensure that it meets or exceeds required legal standards, and we interpret legal process as narrowly as possible. We reject or challenge any requests that have no legal basis or are unclear, over broad, or otherwise inappropriate.

4. Security

a. We have implemented and will maintain the technical and organizational measures that address the (i) security of the Epik Network; (ii) physical security of the facilities; (iii) controls around employee and contractor access to (i) and/or (ii); and (iv) processes for testing, assessing, and evaluating the effectiveness of technical and organizational measures implemented by us.

b. We may make available a number of security features and functionality that Customer may elect to use in relation to the Covered Services. Customer is responsible for (i) properly configuring the Covered Services, (ii) using the controls available in connection with the Covered Services (including the security controls) to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, (iii) using the controls available in connection with the Covered Services (including the security controls) to allow the Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (e.g. backups and routine archiving of Customer Data), and (iv) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

5. Data Subject Rights

Taking into account the nature of the Covered Services, we offer our Customers certain security standards as described herein. Customer may use these stated technical and organizational measures to assist it in connection with its obligations under applicable privacy laws, including its obligations relating to responding to requests from Data Subjects. As commercially reasonable, and to the extent lawfully required or permitted, we shall promptly notify Customer if we directly receive a request from a Data Subject to exercise such rights under any applicable data privacy laws ("Data Subject Request"). In addition, where Customer's use of the Covered Services limits its ability to address a Data Subject Request, we may, where legally permitted and appropriate and upon Customer's specific request, provide commercially reasonable assistance in addressing the request, at Customer's cost (if any). Data Subject Rights are further specified in SCCs incorporated herein.

6. Sub-processing

a. Authorized Sub-processors. Customer agrees that we may use Sub-processors to fulfill its contractual obligations under the Terms of Service and this Addendum or to provide certain services on its behalf, such as providing support services. Customer hereby consents to our use of Sub-processors as described herein.

b. Sub-processor Obligations. Where we use any authorized Sub-processor as described in Section 6.a.:

i. we will restrict the Sub-processor's access to Customer Data only to what is necessary to maintain the Covered Services or to provide the Covered Services to Customer and any end users in accordance with the Covered Services. We will prohibit the Sub-processor from accessing Customer Data for any other purpose;

ii. we will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor is performing the same data processing services that are being provided by us under this Addendum, we will impose on the Sub-processor the same contractual obligations that we have under this Addendum; and

iii. we will remain responsible for its compliance with the obligations of this Addendum and for any acts or omissions of the Sub-processor that cause us to breach any of our obligations under this Addendum.

7. Security Incident

a. Security Incident. If we become aware of a Security Incident, we will, without reasonable undue delay: (i) notify Customer of the Security Incident; and (ii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident in our sole and absolute discretion.

b. Assistance. To assist Customer in relation to any personal data breach notifications Customer is required to make under any applicable privacy laws, we reserve the right but not the obligation to include in any notification outlined herein, such information about the Security Incident as we deem reasonably able to disclose to Customer, taking into account the nature of the Covered Services, the information available to us, and any restrictions on disclosing the information, such as confidentiality.

c. Failed Security Incidents. Customer understands, acknowledges, and agrees that:

i. a failed Security Incident will not be subject to the terms of this Addendum. A failed Security Incident is one that results in no unauthorized access to Customer Data or to any of Epik's Network, equipment, or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents; and

ii. our obligation to report or respond to a Security Incident herein is not and will not be construed as an acknowledgment by us of any fault or liability of Epik with respect to the Security Incident.

d. Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means we select, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on their User Account at all times.

8. Customer Rights

a. Independent Determination. Customer is responsible for reviewing the information made available by us relating to data security and our Security Standards and making an independent determination as to whether the Covered Services meets Customer's requirements and legal obligations as well as Customer's obligations under this Addendum. The information made available is intended to assist Customer in complying with Customer's obligations under the applicable Data Protection Laws.

b. Customer Audit Rights. Customer has the right to confirm our compliance with this Addendum as applicable to the Covered Services. Customer may do so by making a specific request in writing to Legal@Epik.com. This Section will also apply insofar as Epik carries out the control of Sub-processors on behalf of the Customer.

9. Transfers of Personal Data

a. U.S. Based Processing. Customer agrees that, except where specifically noted in the Terms of Service, all Customer Data is processed in the United States. Any transfer outside of the United States will be made in accordance with legally enforceable transfer mechanisms where required by the applicable Data Protection Laws.

b. Application of Standard Contractual Clauses. The Standard Contractual Clauses will apply to Customer Data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognized by the European Commission as providing an adequate level of protection for personal

data (as described in the GDPR). The Standard Contractual Clauses will not apply to Customer Data that is not transferred, either directly or via onward transfer, outside the EEA. Notwithstanding the foregoing, the Standard Contractual Clauses will not apply where the data is transferred in accordance with a recognized compliance standard for the lawful transfer of Personal Data outside the EEA, such as when necessary for the performance of Covered Services pursuant to the Terms of Service.

c. With respect to Customer Data transferred from the United Kingdom for which United Kingdom law (and not the law in any EEA jurisdiction) governs the international nature of the transfer, and such law permits use of the UK SCCs but not use of the SCCs, the UK SCCs form part of this DPA and take precedence over the rest of this DPA, as set forth in the UK SCCs, until such time that the United Kingdom adopts new Standard Contractual Clauses, in which case new, Standard Contractual Clauses will control. For purposes of the UK SCCs, they shall be deemed completed as follows:

i. The "exporters" and "importers" are the Parties and their Affiliates to the extent any of them is involved in such transfer, including those set forth in Annex I.A of the SCCs.
ii. Clause 9 of the UK SCCs specifies that United Kingdom law will govern the UK SCCs.
iii. The content of Appendix 1 of the UK SCCs is set forth in Annex I of the SCCs herein.
iv. The content of Appendix 2 of the UK SCCs is set forth in Annex II of the SCCs herein.

10. Termination of the Addendum

This Addendum will continue in force until the termination of our processing in accordance with the Terms of Service (the "Termination Date").

11. Return or Deletion of Customer Data

Any deletion of Customer Data will be governed by the terms of the particular Covered Services and General Terms of Service.

12. Limitations of Liability

The liability of each party under this Addendum will be subject to the exclusions and limitations of liability set out in the Terms of Service and the applicable SCCs. Customer agrees that any regulatory penalties incurred by us in relation to the Customer Data that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this Addendum and any applicable privacy laws will count towards and reduce our liability under the Terms of Service as if it were liability to the Customer under the Terms of Service.

13. Entire Terms of Service; Conflict

This Addendum supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and us, whether written or oral, regarding the subject matter of this Addendum, including any data processing addenda entered into between us and Customer with regard to the processing of Personal Data and on the free movement of such data. Except as amended by this Addendum, the Terms of Service will remain in full force and effect. If there is a conflict between any other agreement between the parties including the Terms of Service and this Addendum, the terms of this Addendum will control. In the event of a conflict between any provision of the SCCs and any provision of this DPA, this DPA will control to the extent of conflicts.

Appendix 1

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 1.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 1.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 1.b.

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

Clause 2
Effect and invariability of the Clauses

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

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

Clause 3
Third-party beneficiaries

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

i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

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

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

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

v. Clause 13;

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

vii. Clause 16(e);

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

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

Clause 4
Interpretation

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

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

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

Clause 5
Hierarchy

a. 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 transfers

a. 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 1.b.

Clause 7
Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.a.

b. Once it has completed the Appendix and signed Annex 1.a., the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex 1.a.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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 organizational 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

a. The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1.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 annex 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 2 and personal data, the data exporter may redact part of the text of the annex 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 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 1.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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, or unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational measures specified in Annex 2. 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 authorized 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 offenses (hereinafter “Sensitive Data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex 1.b.

8.8 Onward transfers

a. 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 transfers is necessary in order to protect the vital interests of the data subject or of another natural person.

iv. 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 inquiries 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.

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. GENERAL WRITTEN AUTHORIZATION: The data importer has the data exporter's general authorization 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.

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 fulfills 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 fulfill its obligations under that contract.

e. The data importer shall agree to 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 authorized 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 2 the appropriate technical and organizational 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 authorized 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, organization, 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 the above, the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

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

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

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

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

Clause 13
Supervision

a. 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 1.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 inquiries, 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 authorizing 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 authorizing 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 organizational 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 fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational 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 minimization

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

The Parties agree that these Clauses shall be governed by the law of Belgium.

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 Belgium.

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

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

ANNEX 1

DETAILS OF THE PROCESSING

A. LIST OF PARTIES

Data exporter(s): The Data Exporter is the entity identified as "Customer" in the Addendum that has entered the Terms of Service with Epik, and their contact details are as provided by them while subscribing to the Terms of Service.

Signature and date: As of the date of Data Exporter's acceptance of Data Importer's Terms of Service, Data Exporter is deemed to have signed the Data Protection Addendum, including these Standard Contractual Clauses in their entirety.

Role: Controller

Data importer(s): Epik LLC

Contact details: Office of the Data Protection Officer – Legal@Epik.com

Activities relevant to the data transferred under these Clauses: Providing the Services to Data Exporter.

Signature and date: As of the date of Data Exporter's acceptance of Data Importer's Terms of Service, Data Importer is deemed to have signed the Data Protection Addendum, including these Standard Contractual Clauses in their entirety.

Role: Processor

B. DESCRIPTION OF TRANSFER

1. Categories of data subjects whose personal data is transferred.

Customer may upload Personal Data in the course of its use of the Covered Services, the extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

- Prospects, customers, business partners, and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners, and vendors
- Employees, agents, advisers, freelancers of Customer (who are natural persons)
- Customer's Users authorized by Customer to use the Covered Services

2. Categories of personal data transferred.

Customer may upload Personal Data in the course of its use of the Covered Services, the type of and extent to which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data of Data Subjects:

- Name
- Address
- Telephone number
- Date of birth
- Email address
- Other data collected that could directly or indirectly identify you.

3. 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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures

Epik does not intentionally collect special categories of data, but the data exporter, at its own discretion, may collect such data. These categories may include racial or ethnic origin, political opinions, philosophical beliefs, trade union membership, health data, or sex data. Data exporter is solely responsible for meeting all obligations regarding the collection, use, and transfer of such data.

4. The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)
Data is transferred on a continuous basis, for the length of the Agreement between the parties.

5. Nature of the processing.

Epik will Process Personal Data as necessary to perform the Covered Services pursuant to the Terms of Services, product-specific agreements, and as further instructed by Customer throughout its use of the Covered Services.

6. Purpose(s) of the data transfer and further processing.

Epik's General Terms of Services, product-specific agreements, and as further instructed by Customer throughout its use of the Covered Services.

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

Personal data shall be retained for the length of time necessary to provide the Covered Services under the Terms of Service, or as otherwise required by applicable law.

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

Epik's sub-processors will process personal data to assist Epik in providing the Covered Services pursuant to the Agreement, for as long as needed for Epik to provide the Covered Services.

C. COMPETENT SUPERVISORY AUTHORITY

1. Identify the competent supervisory authority/ies in accordance with Clause 13
With respect to the SCCs, the parties agree that the competent supervisory authority is the Belgian Data Protection Authority. With respect to the UK SCCs, the competent supervisory authority means the UK Information Commissioner's Office.

ANNEX 2
Security Standards

We are committed to provide the best level of security to our customer. Please know that we consider a number of factors such as best practices, details and circumstances of processing, the severity and risk of a data breach occurrence, and potential impacts on customers. Below are the standards that we've implemented across our operations to ensure the ongoing confidentiality, integrity, availability, and resilience of our processing systems and services ("Security Standards").

1. Confidentiality.

Below are the practices we use to protect the confidentiality of our customer's personal data.

Physical Security

We have physical access controls in place, such as surveillance systems (including alarms, and CCTV monitoring where appropriate). We also implement clean desk policies (locking of unattended computers, locked cabinets, etc.), visitor access management, and shredding/destruction of documents.

Access Control & Prevention of Unauthorized Access

New access to systems is reviewed and approved by management prior to being granted. We perform regular reviews of user accounts and assigned permissions for key systems. We also limit the personnel who may grant, alter, or cancel authorized access to data and resources. We use 2FA (2-factor authentication) where appropriate.

Data Minimization

Data minimization is accomplished by Personal Identifiable Information/Sensitive Personal Information minimization, segregation of data stored by function (we appropriate), logical segregation of data based access rights, and system/product based defined data retention periods for personal data.

Security Testing

We perform regular network and vulnerability scans throughout our system and have an external bounty program to receive vulnerability findings of independent security researchers and implement a fix further on.

2. Integrity of Data.

We focus on a number of ways to ensure the integrity of customer data.

We use industry standard encryption mechanisms for data in transit.

We collect logs which may include access ID, time, diagnostic data, and other relevant activity. Logs are used (i) for providing, securing, managing, measuring, and improving the Epik services, (ii) as directed or instructed by Customer, and/or (iii) for compliance with Epik policies, applicable law, regulation, or governmental request. This may include monitoring the performance, stability, usage, and security of the Epik services.

3. Availability.

We implement appropriate continuity and security measures to maintain the availability of our service, the personal data residing within those services and the ability to timely restore such data, including the following:

- Extensive performance/availability monitoring and reporting for critical systems.
- Incident response program.
- Critical data either replicated or backed up (Cloud Backups/Hard Disks/Database replication etc.).
- Planned software, infrastructure and security maintenance in place (Software updates, security patches etc.).
- Redundant and resilient systems (server clusters, mirrored DBs with geographically remote mirror, high availability setups etc.) located on off-site and/or geographically separated locations. Use of uninterrupted power supplies, fail redundant hardware and network systems.
- Alarm, security systems in place.
- Physical Protection measures in place for critical sites (surge protection, raised floors, cooling systems, fire and/or smoke detectors, fire suppression systems etc.).

- Failover Protection measures in place, including mechanisms designed to address loss of availability of data, including storing copies of data in a different place from where the primary computer equipment processing is located.

4. Data Processing Instructions.

We have established internal privacy policies and agreements to ensure personal data is processed in accordance with industry standards.