Amplitude
201 Third Street, Suite 200
San Francisco, CA 94103

Amplitude, Inc.
Data Processing Addendum for Terms of Service

This Data Processing Addendum for Terms of Service (this "**TOS DPA**") is incorporated into and forms part of the Amplitude Terms of Service, or other written or electronic agreement between Customer and Amplitude, Inc. which governs Customer's use of the Amplitude Services (as applicable, the "**Terms**"). To the extent there is any conflict between the terms of this TOS DPA and the Terms, this TOS DPA will govern.

Definitions

1. In this TOS DPA:

"**Applicable Law**" means all laws, regulations and other legal requirements applicable to either (i) Amplitude as provider of the Amplitude Services or (ii) Customer as user of the Amplitude Services. For example, to the extent applicable, this includes the General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**"), equivalent requirements in the United Kingdom including the Data Protection Act 2018 and the United Kingdom General Data Protection Regulation ("**UK Data Protection Law**"), and the California Consumer Privacy Act and associated regulations ("**CCPA"**).

"**Designated Address**" means Customer's email address in Customer's account information on record.

"**Personal Data**" means any information relating to an identified or identifiable individual, within the meaning of the GDPR (regardless of whether the GDPR applies).

"**Personal Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or other Processing of, or access to, Personal Data.

"**Process**" and "**Processing**" mean any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated 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.

"**Standard Contractual Clauses**" refers to one or both of the following, as the context requires:

- For Personal Data subject to the UK Data Protection Law, the "**2010 Standard Contractual Clauses,"** defined as the clauses issued pursuant to EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec/2010/87/2016-12-17 and completed as described in the "Data Transfers" section below; and

- For Personal Data subject to the GDPR, the "**2021 Standard Contractual Clauses,"** defined as the clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described in the "Data Transfers" section below.

"**Subprocessor**" means a subcontractor engaged by Amplitude for the Processing of Personal Data.

2. For ease of reading, some other terms are defined later in the TOS DPA. Capitalized terms used but not otherwise defined in the TOS DPA will have the meaning set forth in the Terms.

Scope, Relationship of the Parties, and Data Use Limitations

3. This TOS DPA applies only to Personal Data that Customer submits to Amplitude as part of the Amplitude Services, where such data is Customer Data and Amplitude Services as defined in the Terms.

4. Unless required by Applicable Law, Amplitude will Process the Personal Data only to: (i) perform the Amplitude Services for Customer pursuant to the Terms; (ii) comply with this TOS DPA; and (iii) carry out Customer's reasonable written instructions that are consistent with the Terms and this TOS DPA. Without limiting the foregoing, (i) Amplitude shall not "sell" the Personal Data, as such term is defined in the CCPA; and (ii) Amplitude shall not retain, use, or disclose Personal Data outside of the direct business relationship between Customer and Amplitude.

5. If Amplitude receives a demand under Applicable Law to engage in Processing not permitted by the above, Amplitude shall attempt to redirect the demand to Customer and Customer agrees Amplitude may provide information as reasonably necessary for such redirect. If Amplitude cannot redirect the demand to Customer, Amplitude shall, to the extent legally permitted to do so, take commercially reasonable steps to provide Customer reasonable notice of the demand as promptly as possible under the circumstances.

6. For the Amplitude Services, the parties acknowledge and agree that Customer is the "Controller" and Amplitude is Customer's "Processor" as such terms are defined in the GDPR (regardless of whether the GDPR applies).

Confidentiality and Training

7. Amplitude will ensure that the persons Amplitude authorizes to Process the Personal Data are contractually required to maintain the confidentiality of such data. Amplitude will train relevant employees regarding privacy, confidentiality, and data security.

Security

8. Amplitude will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Personal Data, including measures designed to prevent a Personal Data Breach.

Subprocessors

9. Customer acknowledges and agrees that Amplitude may engage Subprocessors in connection with the provision of the Amplitude Services, provided that Amplitude has entered into a written agreement with each Subprocessor containing, in substance, data protection obligations no less protective than those in this TOS DPA with respect to the protection of Personal Data, to the extent applicable to the nature of the Processing provided by such Subprocessor.

10. Current Subprocessors are listed in Schedule C (the "**Subprocessor List"**). When any new Subprocessor is to be engaged, Amplitude will update Schedule C to include the new Subprocessor at least ten (10) business days prior to giving the Subprocessor access to the Personal Data. If Customer would like to receive email notification of such updates, please contact subprocessor.notifications@amplitude.com to subscribe to such updates.

11. Customer may object to Amplitude's use of a new Subprocessor, by notifying Amplitude in writing of such objection within ten (10) business days of Amplitude's notice of the new Subprocessor. If Customer objects to a new Subprocessor for the Amplitude Services, as permitted in the preceding sentence, Customer's sole remedy is to cease use of the Amplitude Services.

12. Amplitude remains liable for its Subprocessors' acts and omissions to the same extent Amplitude is liable for its own, consistent with the limitations of liability set forth in the Terms or this TOS DPA.

13. The parties agree that any audit rights provided under the terms of this TOS DPA do not extend to Amplitude's Subprocessors' facilities.

Assistance Responding to Individuals' Requests to Exercise Rights

14. Amplitude will reasonably and timely assist Customer with the fulfillment of Customer's obligation to honor and respond to requests by individuals to exercise their Personal Data-related rights under the GDPR or other Applicable Law (a "**Data Subject Request**"), such as rights to access, correct, or delete their Personal Data, insofar as technically possible.

15. If Amplitude receives a Data Subject Request or a complaint from an individual or their representative and the communication identifies Customer (or if Amplitude is aware that the communication pertains to the Personal Data Amplitude Processes for Customer), Amplitude will take commercially reasonable steps to forward the communication to Customer at the Designated Address.

Personal Data Breach Notification

16. Amplitude will comply with the Personal Data Breach-related obligations applicable to it under the GDPR and other Applicable Law. Amplitude will assist Customer in complying with those applicable to Customer by informing Customer of a Personal Data Breach without undue delay.

17. Amplitude will provide such notification in accordance with Applicable Law to Customer at the Designated Address.

18. Such notification shall not be construed as an acknowledgement of fault or responsibility and the obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

19. Amplitude shall make reasonable efforts to identify the cause of such Personal Data Breach and take such steps as Amplitude deems necessary and reasonable to remediate the cause of such Personal Data Breach to the extent the remediation is within Amplitude's reasonable control.

Assistance with DPIAs and Consultation with Supervisory Authorities

20. To the extent Customer does not otherwise have access to the relevant information and to the extent such information is available to Amplitude, Amplitude will provide reasonable assistance to and cooperation with Customer for (i) Customer's performance of any data protection impact assessment of the Processing or proposed Processing of the Personal Data involving Amplitude, and (ii) related consultation with supervisory authorities, either or both of which Customer reasonably considers to be required of Customer by Applicable Law.

Data Return and Destruction

21. Amplitude will destroy all Personal Data within 90 days of Customer providing notice of termination of the Terms (including on all Subprocessor systems) in accordance with the Terms, except to the extent Applicable Law or other law requires storage of the Personal Data or retention of the Personal Data by Amplitude is necessary to resolve a dispute between the parties.

22. If requested by Customer in writing within 10 days after the termination of these Terms, Amplitude will first return a copy of the Personal Data to Customer in any reasonably requested format before the destruction described above.

Compliance Verification and Audits

23. Amplitude is audited annually against known, established industry standards.

24. Upon Customer's written request and at its own expense, Amplitude will also allow for Customer's

audit of Amplitude's applicable controls, including inspection of Amplitude's physical facility, provided such audit is i) required by a Supervisory Authority or other similar regulatory authority responsible for the enforcement of Applicable Law; ii) conducted by Customer or a third party auditor designated by Customer that has executed an appropriate confidentiality agreement with Amplitude, and iii) Customer and Amplitude mutually agree on the details of the audit, including the reasonable start date, scope and duration of, and security and confidentiality controls applicable to such audit.

Data Transfers

25. If in the performance of the Amplitude Services Amplitude makes an international transfer of Personal Data, Customer authorizes such transfer and the transfer mechanisms listed below shall apply, as applicable.

26. To the extent required under UK Data Protection Law,

    a. the 2010 Standard Contractual Clauses form part of this TOS DPA and take precedence over the rest of this TOS DPA to the extent of any conflict, and they will be deemed completed as follows:

        i. The "exporter" is the Customer, and the exporter's contact information is set forth in Schedule A below.

        ii. The "importer" is Amplitude, and Amplitude's contact information is set forth in Schedule A below.

        iii. Where Clause 9 of the 2010 Standard Contractual Clauses requires specification of the law that governs the 2010 Standard Contractual Clauses, the Parties select the law of the United Kingdom.

        iv. The "illustrative indemnification clause" labeled "optional" does not apply.

        v. Appendices 1 and 2 of the 2010 Standard Contractual Clauses are set forth in Schedule A below.

        vi. By entering into this TOS DPA, the Parties are deemed to be signing the 2010 Standard Contractual Clauses and its applicable Appendices.

27. To the extent otherwise legally required, the 2021 Standard Contractual Clauses form part of this TOS DPA and take precedence over the rest of this TOS DPA to the extent of any conflict, and they will be deemed completed as follows:

    a. Customer acts as controller and Amplitude acts as Customer's processor with respect to the Personal Data subject to the 2021 Standard Contractual Clauses, and its Module 2 (Controller to Processor) applies.

    b. Clause 7 (the optional docking clause) does not apply.

    c. Under Clause 9 (Use of subprocessors), the parties select Option 2 (General written authorization). The current list of Subprocessors is set forth below in Schedule C of this TOS DPA. Amplitude shall update the list at least ten (10) business days in advance of any intended additions or replacements of subprocessors.

    d. Under Clause 11 (Redress), the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply.

    e. Under Clause 17 (Governing law), the parties choose Option 1 (the law of an EU Member State that allows for third-party beneficiary rights). The parties select the law of the Netherlands.

f. Under Clause 18 (Choice of forum and jurisdiction), the parties select the courts of the Netherlands.

g. Annexes I and II of the 2021 Standard Contractual Clauses are set forth in Schedule B of the TOS DPA.

h. Annex III of the 2021 Standard Contractual Clauses (Subprocessor List) is set forth in Schedule C of the TOS DPA.

Miscellaneous

28. This TOS DPA survives termination of the Terms or so long as Amplitude continues to Process such Personal Data or until such Personal Data has been deleted or returned to Customer.

29. If there is a conflict between any provision of the Terms and this TOS DPA, this TOS DPA shall control.

30. Notwithstanding anything to the contrary in the Terms or this TOS DPA, each party's liability, taken together in the aggregate, arising out of or relating to this TOS DPA, the SCCs, and any other data protection agreements signed by the parties ("**Ancillary Agreement**") in connection with the Terms (if any), whether in contract, tort, or under any other theory of liability, is subject to the limitations on liability section in the Terms, and any reference in such section to the liability of a party means the total aggregate liability of that party under the Terms, this TOS DPA and Ancillary Agreement (if any) together.

31. This TOS DPA supersedes and replaces all previous written and oral agreements, communications and other understandings related to the subject matter of this TOS DPA.

Schedule A to TOS DPA
Appendices 1 and 2 to the 2010 Standard Contractual Clauses

APPENDIX 1 TO THE 2010 STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): The data exporter is the legal entity subject to the Terms as Customer, and who is engaging Amplitude to provide the cloud-based digital optimization services, defined in the Terms as "Amplitude Services."

Data importer

The data importer is (please specify briefly activities relevant to the transfer): The data importer is Amplitude, the provider of the Amplitude Services, as defined in the Terms. Amplitude's entity and contact details are set forth in the Terms.

Data subjects

The Personal Data transferred concern the following categories of data subjects (please specify):

Customer may submit Personal Data to the Amplitude Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include the Personal Data of Customer's end users of mobile and web applications, as well as Customer's authorized users of the Amplitude Services.

Categories of data

The Personal Data transferred concern the following categories of data (please specify):

Customer may submit Personal Data to the Amplitude Services, the extent of which is determined and controlled by Customer in its sole discretion and may include the following categories of Personal Data:

- information about end users (e.g., names, email addresses, and telephone numbers) and their website and application browsing activity, history, location, and device information (e.g., device identifiers (not Apple ID), operating system, and IP addresses); and
- information about Customer's users and device information.

Special categories of data (if appropriate)

The Personal Data transferred concern the following special categories of data (please specify): None, unless the Terms specifically permit the transfer of such data.

Processing operations (including subject matter, nature, purpose and duration of Processing)

The Personal Data transferred will be subject to the following basic processing activities (please specify):

Amplitude will Process Personal Data in its performance of the Amplitude Services pursuant to the Terms and this TOS DPA, as deemed requested and instructed by Customer by acceptance of the Terms, creation of an Amplitude account, or use of or access to the Amplitude Services.

APPENDIX 2 TO THE 2010 STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Amplitude, the data importer, will implement and maintain administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data uploaded to the Amplitude Services by Customer, the data exporter. For a description of these technical and organizational security measures, see Schedule B, Annex II.

Schedule B to the TOS DPA
Annexes I and II of the 2021 Standard Contractual Clauses

ANNEX I

A. LIST OF PARTIES

MODULE TWO: Transfer controller to processor

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

The data exporter is the legal entity subject to the Terms as Customer, and who is engaging Amplitude to provide the cloud-based digital optimization services, defined in the Terms as "Amplitude Services."

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]

The data importer is Amplitude, the provider of the Amplitude Services, as defined in the Terms. Amplitude's entity and contact details are set forth in the Terms.

B. DESCRIPTION OF TRANSFER

MODULE TWO: Transfer controller to processor

Categories of data subjects whose personal data is transferred:

Customer may submit Personal Data to the Amplitude Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include the Personal Data of Customer's end users of mobile and web applications, as well as Customer's authorized users of the Amplitude Services.

Categories of personal data transferred:

Customer may submit Personal Data to the Amplitude Services, the extent of which is determined and controlled by Customer in its sole discretion and may include the following categories of Personal Data:

- information about end users (e.g., names, email addresses, and telephone numbers) and their website and application browsing activity, history, location, and device information (e.g., device identifiers (not Apple ID), operating system, and IP addresses); and
- information about Customer's users and device information.

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:

No sensitive data shall be submitted to the Amplitude Services, unless the Terms specifically permit the transfer of such data.

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

Notwithstanding termination of the Terms, Amplitude will Process Customer Personal Data continuously, until deletion of all Customer Personal Data as described in this TOS DPA.

Nature of the processing:

Amplitude will Process Personal Data in its performance of the Amplitude Services pursuant to the Terms and this TOS DPA, and to comply with Customer's request and instruction to do so provided by Customer's acceptance of the Terms, creation of an Amplitude account, or use of or access to the Amplitude Services.

Purpose(s) of the data transfer and further processing:

Customer may submit Personal Data to the Amplitude Services, the extent of which is determined and controlled by Customer in its sole discretion, for Amplitude's provision of the Amplitude Services, as described in the Terms and further documented, reasonable instructions from Customer specifically agreed upon by the parties.

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

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

The period for which Customer's Personal Data will be retained in the Amplitude Services is determined by Customer during the term of the relationship. Upon termination of the Terms, Customer may retrieve or delete its Personal Data as set forth in the Terms and this TOS DPA and Amplitude will destroy (including on all Subprocessor systems) Customer's Personal Data within the timeline described in this TOS DPA.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE TWO: Transfer controller to processor

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

Where Customer is established in an EU Member State, Customer shall maintain accurate records of the applicable Member State(s) and competent supervisory authority, which shall be made available to Amplitude upon request. Where Customer is not established in an EU Member State, the supervisory authority of the Netherlands shall act as the competent supervisory authority for these SCCs.

ANNEX II

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

Amplitude, the data importer, maintains administrative, physical and technical safeguards for the protection of the security, confidentiality and integrity of Personal Data uploaded to the Amplitude Services by Customer, the data exporter. Amplitude's information security program is designed in accordance with ISO 27001, an industry recognized gold standard and is described in more detail below. Amplitude may review and update these security standards from time to time.

Amplitude's security controls are designed to address its posture as a cloud-based platform as a service (PaaS) provider. The following concepts apply to Amplitude's platform and its provision of the Amplitude Services and are contextually important to understanding Amplitude's security controls.

Amplitude is data neutral and data agnostic: The Amplitude PaaS does not know what data customers choose to send to the platform and will process all data regardless of its nature as long as it fits the predefined characteristics that allow it to be processed. Amplitude does not make any data-based decisions other than following customers' instructions as they configure the platform to perform their desired operations. Once data is processed by the Amplitude platform, it is stripped of unnecessary information, and made computationally difficult to separate into the original event state. Recovering a structured dataset tied to a specific individual is computationally difficult.

No employee access: Amplitude employees do not directly access customer Personal Data as part of their normal job duties, except as necessary to provide the Amplitude Services or to provide support to a customer upon a customer's request. Only the Amplitude platform interacts with such data, and only according to the programmatic instructions provided by each Amplitude customer with respect to its data.

Data immutability: Customer raw data feeds are preserved in their original state, in encrypted form, in customer-specific S3 buckets, and Customer Data is logically separated using multiple techniques.

Security Program: Amplitude's PaaS is designed according to established industry best security practices, and includes many technical and administrative security controls, including, without limitation:

- Audits and Certifications: Amplitude's information security program is assessed annually by independent third-party auditors.
- Secure Data Centers: Amplitude's PaaS is fully embedded within Amazon's AWS platform. For more information about Amazon's AWS security, refer to https://aws.amazon.com/security/.
- Information Security Policy: Amplitude has developed and implemented, and will maintain, security policies that govern all relevant aspects of its security program.
- Encryption:
    - Amplitude maintains a secure environment for the transmission of customers' Personal Data, utilizing encryption consistent with industry standard practices and utilizing industry accepted encryption technologies.
    - Amplitude maintains a secure environment for the storage of customers' Personal Data, utilizing encryption consistent with industry standard practices.
- Access Controls:
    - Amplitude personnel access the Amplitude PaaS via unique user IDs, and are required to authenticate through VPN and multi-factor authentication.
    - Amplitude personnel access customer Personal Data as necessary to provide the Amplitude Services under the Terms, to provide customer support upon a customer's request, or to comply with the law or a binding order of a governmental body.
- Vulnerability Detection and Management:
    - Anti-Virus and Vulnerability Detection: Amplitude leverages threat detection tools to monitor and alert Amplitude to suspicious activities, potential malware, viruses and/or malicious

computer code (collectively, "Malicious Code"). Amplitude does not monitor Customer Data for Malicious Code.
    - Penetration Testing and Vulnerability Detection: Amplitude regularly conducts penetration tests throughout the year and engages one or more independent third parties to conduct penetration tests of the Services at least annually.
    - Vulnerability Management: Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on their potential impact to the Amplitude Services.
- Endpoint Controls: Amplitude logically separates its endpoints and end user environment from its PaaS environment. Multi-factor authentication is required to access the AWS environment.
- Monitoring and Logging: Amplitude monitors its PaaS environment 24/7/365 and centralizes its logs. Anomalies are investigated and prioritized on a 24/7/265 basis.
- Program Testing: Amplitude regularly tests and evaluates its security program.
- Administrative Controls:
    - Personnel Security: Amplitude requires criminal background screening on its personnel as part of its hiring process, to the extent permitted by Applicable Law.
    - Personnel Training: Amplitude maintains a documented awareness and training program for its personnel, including but not limited to onboarding and annual training.
    - Personnel Agreements: Amplitude personnel are required to sign confidentiality agreements and to acknowledge Amplitude's Information Security Policy.
    - Personnel Access Reviews and Separation: Amplitude reviews the access privileges of its personnel to the Amplitude PaaS at least quarterly, and removes access on a timely basis for all separated personnel.
- Physical & Environmental Controls:
    - Data Centers: Amplitude hosts all Customer Data in Amazon AWS. Amplitude regularly reviews Amazon's physical and environmental controls for its relevant data centers, as audited by Amazon's third-party auditors. Such controls include, but are not limited to:
        - Physical access to the facilities is controlled at the building ingress points;
        - Visitors are required to present ID and are signed in;
        - Physical access to servers is managed by access control devices;
        - Physical access privileges are reviewed regularly;
        - Facilities utilize monitor and alarm procedures;
        - Fire detection and protection systems;
        - Power back-up and redundancy systems; and
        - Climate control systems.
    - Amplitude Corporate Offices: While Customer Data is not hosted at Amplitude's corporate offices, Amplitude's technical, administrative, and physical controls for its corporate offices are covered by its ISO 27001 certification and include, but are not limited to, the following:
        - Physical access to the corporate offices is controlled at office ingress points;
        - Badge access is required for all personnel and badge privileges are reviewed regularly;
        - Visitors are required to sign in;
        - Tagging and inventory of Amplitude-issued laptops and network assets;
        - Fire detection and sprinkler systems; and
        - Climate control systems.
- Incident Detection and Response: Amplitude's incident response process is designed to address all legal, contractual, and regulatory requirements.
    - Security Incident Reporting: If Amplitude becomes aware of a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data ("Security Incident"), Amplitude will notify impacted customers in accordance with the terms of this TOS DPA.
    - Investigation: In the event of a Security Incident, Amplitude shall take reasonable steps to contain, investigate, and mitigate any Security Incident.
    - Communication and Cooperation: Amplitude's notice to impacted customers shall include, but not be limited to, the nature and likely consequences of the Security Incident, the measures taken and/or proposed by Amplitude to mitigate or contain the Security Incident,

and, where possible, the categories and approximate number of data records concerned. Communications by or on behalf of Amplitude in connection with a Security Incident are not an acknowledgement by Amplitude of fault or liability with respect to the Security Incident.

Schedule C to the TOS DPA
Subprocessor List

Subprocessor	Purpose	Location	Transfer Mechanism
Amazon Web Services	Cloud hosting and infrastructure provider	United States Germany	SCCs N/A
Snowflake Computing, Inc.	Data warehousing services (if applicable)	United States	SCCs
Intercom	In-application customer support	United States	SCCs
LogRocket	Customer support	United States	SCCs
Sentry	Error logging	United States	SCCs