Data Processing Addendum

This Data Processing Addendum ("**Addendum**") forms an integral part of the Agreement between Customer and Company and applies to the extent that Company processes Personal Data, or has access to Personal Data, in the course of its performance under the Agreement, as specified in **Appendix 1**, which is attached and incorporated hereto by reference.

Customer shall qualify as the Data Controller and Company shall qualify as the Data Processor, as this term is defined under Data Protection Law. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

1. Definitions
    a. "**Approved Jurisdiction**" means a member state of the EEA, or other jurisdiction as may be approved as having adequate legal protections for data by the European Commission.
    b. "**CCPA**" means the California Consumer Privacy Act Cal. Civ. Code § 1798.100 et seq.
    c. "**Data Controller**", "**Data Processor**", "**Personal Data Breach**", "**data subject**", "**process**", "**processing**" and "**sell**" shall have the meanings ascribed to them in the Data Protection Law. Where applicable, Data Controller shall be deemed to be a "Business", Data Processor shall be deemed to be a "Service Provider", and "data subject" shall be deemed to be a "Consumer" as these terms are defined under the CCPA.
    d. **"EEA"** means those countries that are member of the European Economic Area.
    e. "**Data Protection Law**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (General Data Protection Regulation) ("**GDPR**") and the CCPA.
    f. "**Personal Data**" means any information which (i) can be related to an identifiable individual, including any information that can be linked to an individual or used to directly or indirectly identify an individual, **and** (ii) supplied by Customer to Company pursuant to the Agreement or which Company generates, collects, stores, transmits, or otherwise processes on behalf of Customer in connection with the Agreement. Personal Data may include information which is related to Customer's end users, employees, contractors, suppliers and other third parties.
    g. "**Security Measures**" mean commercially reasonable security-related policies, standards, and practices commensurate with the size and complexity of Company's business, the level of sensitivity of the data collected, handled and stored, and the nature of Company's business activities.
    h. **"Standard Contractual Clauses"** mean the standard contractual clauses for the transfer of personal data to data processors established in third countries adopted by the European Commission Decision EC/2010/87: 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.
    i. "**Sub-Processors**" mean any affiliate, agent or assign of Company that may process Personal Data pursuant to the terms of the Agreement, and any unaffiliated processor engaged by Company.
2. Compliance with Laws
    a. Each Party shall comply with its respective obligations under the Data Protection Law.
    b. Company shall provide reasonable cooperation and assistance to Customer in relation to Company's processing of Personal Data in order to allow Customer to comply with its obligations as a Data Controller under Data Protection Law.

c. Company agrees to notify Customer promptly if it becomes unable to comply with the terms of this Addendum and take reasonable and appropriate measures to remedy such non-compliance.
d. Throughout the duration of the Addendum, Customer agrees and warrants that:
    i. the processing of Personal Data by Customer, as well as any instruction to Company in connection with the processing of Personal Data, has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Law;
    ii. Personal Data has been collected and transferred fairly and lawfully, pursuant to any applicable Data Protection Law, and that the concerned data subjects have been informed of the processing and transfer of Personal Data pursuant to this Addendum.

3. Obligations under the CCPA
    a. Company shall not sell the Personal Data.
    b. Company is prohibited from retaining, using or disclosing Personal Data for a commercial purpose other than providing the services to the Customer under the Agreement and from retaining, using or disclosing the Personal Data outside of the Agreement.
    c. Company understands its obligations under this section and will comply with them.

4. Processing Purpose and Instructions

    a. The subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, shall be as set out in the Agreement.
    b. The duration of the processing under the Agreement is determined by the Parties, as set forth in the Agreement.
    c. Company shall process Personal Data only to deliver the Services in accordance with Customer's written instructions, the Agreement and the Data Protection Law, unless Company is otherwise required by law to which Company is subject (and in such a case, Company shall inform Customer of that legal requirement before processing, unless that law prohibits such information disclosure on grounds of public interest).
    d. Processing any Personal Data outside the scope of the Agreement will require prior written agreement between Company and Customer by way of written amendment to the Agreement and will include any additional fees that may be payable by Customer to Company for carrying out such instructions.

5. Reasonable Security and Safeguards

    a. Company represents, warrants, and agrees to use the Security Measures as set out in **Appendix 2** to (i) protect the availability, confidentiality, and integrity of any Personal Data collected, accessed, used, or transmitted by Company in connection with this Agreement, and (ii) protect such data from Personal Data Breach incidents.
    b. The Security Measures are subject to technical progress and development and Company may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services subscribed by Customer.
    c. Company shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision who have access to and process Personal Data. Company shall ensure that

persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d. Customer is responsible for using and configuring the Services in a manner which enables Customer to comply with Data Protection Law, including implementing appropriate technical and organizational measures.

6. Personal Data Breach

Upon becoming aware of a Personal Data Breach, Company will notify Customer without undue delay and will provide information relating to the Personal Data Breach as reasonably requested by Customer. Company will use reasonable endeavors to assist Customer in mitigating, where possible, the adverse effects of any Personal Data Breach.

7. Security Assessments and Audits

a. Company shall, upon reasonable and written notice and subject to obligations of confidentiality, allow its data processing procedures and documentation to be inspected no more than once a year by Customer (or its designee) in order to ascertain compliance with this Addendum. Company shall cooperate in good faith with audit requests by providing access to relevant knowledgeable personnel and documentation.

b. At Customer's written request, and subject to obligations of confidentiality, Company may satisfy the requirements set out in this section by providing Customer with a copy of a written report so that Customer can reasonably verify Company's compliance with its obligations under this Addendum.

8. Cooperation and Assistance

a. If Company receives any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement, including requests from individuals seeking to exercise their rights under Data Protection Law, Company will promptly redirect the request to Customer. Company will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Company is required to respond to such a request, Company will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so.

b. If Company receives a legally binding request for the disclosure of Personal Data which is subject to this Addendum, Company shall (to the extent legally permitted) notify Customer upon receipt of such order, demand, or request. Notwithstanding the foregoing, Company will cooperate with Customer with respect to any action taken pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data.

c. Upon reasonable notice, Company shall provide reasonable assistance to Customer in:
    i. allowing data subjects to exercise their rights under the Data Protection Law;
    ii. ensuring compliance with any notification obligations of Personal Data Breaches to the supervisory authority and communication obligations to data subjects, as required under Data Protection Law;

iii. Ensuring compliance with its obligation to carry out Data Protection Impact Assessments ("**DPIA**") or prior consultations with data protection authorities with respect to the processing of Personal Data. Any assistance to Customer with regard to DPIA or prior consultations will be solely at Customer's expense.

9. Use of Sub-Processors
    a. Customer provides a general authorization to Company to appoint (and permit each Sub-Processor appointed in accordance with this section to appoint) Processors and/or Sub Processors in accordance with this section.
    b. Company may continue to use those Processors and/or Sub Processors already engaged by Company as at the date of this Agreement, subject to Company in each case as soon as practicable meeting the obligations set out in this section. A list of the Company's current Sub Processors is attached as Appendix 3.
    c. Company can at any time and without justification appoint a new Processor and/or Sub-Processor provided that Company provides seven (7) days' prior notice and the Customer does not legitimately object to such changes within that timeframe. Legitimate objections must contain reasonable and documented grounds relating to a Processor and/or Sub-Processor's non-compliance with Data Protection Law. If, in Company's reasonable opinion, such objections are legitimate, Company shall either refrain from using such Processor and/or Sub-Processor in the context of the processing of Personal Data or shall notify Customer of its intention to continue to use the Processor and/or Sub-Processor. Where Company notifies Customer of its intention to continue to use the Processor and/or Sub-Processor in these circumstances, Customer may, by providing written notice to Company, terminate the Agreement immediately.
    d. With respect to each Processor and/or Sub Processor, Company shall ensure that the arrangement between Company and the Processor and/or Sub Processor is governed by a written contract including terms which offer at least the same level of protection as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR.
    e. Company will be responsible for any acts, errors or omissions by its Sub-Processors, which may cause Company to breach any of its obligations under this Addendum.

10. International Data Transfers
    a. To the extent that Company processes Personal Data outside the EEA, then the Parties shall be deemed to enter into the Standard Contractual Clauses, which are incorporated herein by reference, in which event the Customer shall be deemed as the Data Exporter and the Company shall be deemed as the Data Importer (as these terms are defined therein);
    b. Company may transfer Personal Data of residents of the EEA or Switzerland outside the EEA ("**Transfer**"), only subject to the following: The Transfer is necessary for the purpose of Company carrying out its obligations under the Agreement, or is required under applicable laws; and the Transfer is done in accordance with Data Protection Law.

11. Data Retention and Destruction

Company will only retain Personal Data for the duration of the Agreement or as required from its obligations under the Agreement. Following expiration or termination of the Agreement, Company will delete or return to Customer all Personal Data in its possession as provided in the Agreement except to the extent Company is required under applicable law to retain the Personal Data (in which case Company will implement

reasonable measures to prevent the Personal Data from any further processing). The terms of this Addendum will continue to apply to such Personal Data.

12. General

a. Any claims brought under this Addendum will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement.
b. In the event of a conflict between the Agreement (or any document referred to therein) and this Addendum, the provisions of this Addendum shall prevail.
c. Company may change this Addendum if the change is required to comply with Data Protection Law, a court order or guidance issued by a governmental regulator or agency, provided that such change does not: (i) seek to alter the categorization of the Company as the Data Processor; (ii) expand the scope of, or remove any restrictions on, either Party's rights to use or otherwise process Personal Data; or (iii) have a material adverse impact on Customer, as reasonably determined by Company.
d. If Company intends to change this Addendum under this section, and such change will have a material adverse impact on Customer, as reasonably determined by Company, then Company will use commercially reasonable efforts to inform Customer at least 30 days (or such shorter period as may be required to comply with applicable law, applicable regulation, a court order or guidance issued by a governmental regulator or agency) before the change will take effect.

_____	_____
Logshero Ltd	Customer- [_____]
By: _____	By: _____
Title: _____	Title: _____
Date: _____	Date: _____

Appendix 1

If the Standard Contractual Clauses apply, then this Appendix is completed in accordance with Clause 2 of the Standard Contractual Clauses and forms an integral part of the Standard Contractual Clauses.

Details of the Data Exporter
Data Exporter is the Customer

Details of the Data Importer
Data Importer is the Company

Governing law
With reference to Clause 9 and Clause 11(3) of the Standard Contractual Clauses, the Standard Contractual Clauses shall be governed by the law of the Agreement.

Data exporter and data importer activities relevant to the transfer
Activities relevant to the transfer include the performance of the Services for Customer, as contemplated in the Agreement.

Duration of the data processing
The duration of the data processing shall be throughout the duration of the Agreement.

The Data may concern the following categories of data subjects
Data subjects whose Personal Data may be included within Customer's data logs

The Data may concern the following categories of data which relate to data subjects:

- Name;
- Email address;
- IP address;
- Any Personal Data which is obtained in Customer's log data.

Special Categories of Data
The Data Exporter will not share any special categories of Data

Purpose of processing operations

- Tagging Customer's log data (which may include Personal Data) to identify specific end users and enrich log data with additional metadata.
- Indexing Customer's log data (which may include Personal Data) into a dedicated data-store that is able to scale and grow to fit any needed capacity of log data.
- Providing analytics services on the processed log data and allowing Customer to perform activities concerning such data (e.g. create searches, visualizations, dashboards, and alerts).

Appendix 2

Description of the technical and organizational security measures implemented by Company (If the Standard Contractual Clauses apply, then this Appendix is completed in accordance with Clauses 4(d) and 5(c)):

1. Internal R&D Processes

Security-oriented environments start with high coding standards that guard against attempted security breaches and are accompanied by rigorous code reviews and tests. Company employs strict development processes and coding standards to ensure that both adhere to best industry security practices. In addition, the Company's testing platform performs a set of various black box and white box tests for quality assurance (including ongoing penetration tests). R&D processes are implemented and supported with security as a top priority across all system layers, from the physical layers up to the application layer. The R&D source code is monitored by a best-of-breed security vulnerability identification service. In addition to the R&D processes, the Company performs periodical mandatory security training to all its employees.

2. Physical Data Center Security

Company relies on the AWS/Azure exceptionally flexible and secure cloud infrastructure to store data logically across multiple AWS/Azure cloud regions and availability zones. AWS/Azure abide by industry and government requirements and ensures the utmost in data security and protection. These may include: SOC 1, SOC2, SOC3, SSAE 16 / ISAE 3402, FISMA, DIACAP, FedRAMP and others.

All data centers that run Company's platform are secured and monitored 24/7, and physical access to AWS/Azure facilities is strictly limited. (For more information, see: http://aws.amazon.com/security or https://azure.microsoft.com/en-in/product-categories/security/)

3. Instance and Network Security

Every microservice runs inside a well-defined Docker container that allows specific levels of access to select controllers. Company uses Docker to avoid erroneous instance-configuration changes, upgrades, and corruption that are common sources of security breaches. Additionally, the Company hardens docker images running within containers to enable various network access controls.

Company takes all necessary precautions to ensure that every layer involved in data transfer is secured by best-of-breed technologies. The Company's network is segmented using AWS/Azure security groups and additional custom measures. In addition, the Company monitors security alerts that are analyzed and addressed in real-time. Through in-depth network monitoring, Company is able to detect anomalies and take a proactive approach to eliminating potential breaches.

4. Customer Data Security

Company secures each and every step of the data funnel. Company dedicates logical segments of the data stores for each individual customer's data logs, ensuring full data-segregation. Data is tagged, segregated, and tunneled through the Company's data-ingestion system. They mark each specific piece of given customer data according to its associated organization, which is associated with that data throughout its life cycle. When data is in transit in Company's ingestion pipeline, it is marked with specific information, including its associated customer, so that it can only be accessed by that customer. The Company supports TLS v1.2 encryption for data in transit over the internet, so customers can securely upload their data to the Company cloud and securely browse through their own Company console. Cold data is encrypted and hosted in separate Simple Storage Service (S3) buckets, which are secured via durable AES 256-bit encryption.

In addition, Company continuously tracks and maintains the location and state of their customers' data.

5. Access Management

Company supports role-based access through their interface, allowing end users to be defined as admins or users as well as suspended or deleted. Customers' account administrators manage and control user access, including provisioning new end users with a defined access level.

6. Auditing

To verify adherence with compliance policies, Company uses 3rd-party auditing services. E&Y, one of the "Big Four" auditing firms, performs periodic and comprehensive auditing to audit and validate processes.

7. Compliance

The Company has the following compliance certifications in place: SOC 2- type II; ISO 27001; PCI level 1 service provider.

Appendix 3

List of current Sub Processors

Sub Processor	Place of Processing	Sub Processing Activities
Amazon Web Service	TBD by Customer, according to the available locations	Hosting Services
Microsoft Azure	TBD by Customer, according to the available locations	Hosting Services
Akamai Technologies Inc.		CDN (Content Delivery Network) DNS (Domain Name System) WAF (Web Application Firewall)
Logz.io, Inc.	US	Company's affiliate (wholly owned US subsidiary, under an inter-company DPA)
Logz.io UK Limited	UK	Company's affiliate (wholly owned UK subsidiary, under an inter-company DPA)