Data Processing Addendum

This Data Processing Addendum ("**Addendum**") forms an integral part of the Service Agreement ("**Agreement**") between _____("**Customer**") and Coralogix Inc. 535 Mission, San Francisco, CA (**"Company**") and applies to the extent that the Company Processes Personal Data, or has access to Personal Data, on behalf of the Customer, in the course of its performance under the Agreement.

Company shall qualify as the Data Processor, as this term is defined under Data Protection Legislation.

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 pursuant to the applicable Data Protection Legislation as having adequate legal protections for data by the European Commission.
    b. "**Breach Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
    c. **"Data Protection Legislation**" means any and/or all applicable domestic and foreign laws, rules, directives and regulations, on any local, provincial, state or deferral or national level, pertaining to data privacy, data security and/or the protection of Personal Data, including the Data Protection Directive 95/46/EC and the Privacy and Electronic Communications Directive 2002/58/EC (and respective local implementing laws) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), including any amendments or replacements to them, including the 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 ("**GDPR**").
    d. "**Data Controller**", "**Data Processor**", "**Data Subject**", "**Personal Data**", "**Process**" and "**Processing**" shall have the meanings ascribed to them in the Data Protection Legislation.
    e. **"EEA**" means those countries that are member of the European Economic Area.
    f. "**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.

g. "**Sub-Processors**" mean any Affiliate, agent or assignee 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 Legislation.
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 the Data Protection Legislation.
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. Personal Data has been and will continue to be collected, processed and transferred by Customer in accordance with the relevant provisions of the Data Protection Legislation;
    ii. the processing of Personal Data by Customer, as well as any instruction to Company in connection with the processing of the Personal Data ("**Processing Instructions**"), has been and will continue to be carried out in accordance with the relevant provisions of the Data Protection Legislation; and that
    iii. The Customer has informed Data Subjects of the processing and transfer of Personal Data pursuant to the Addendum and obtained the relevant consent thereto (including without limitation any consent required in order to comply with the Processing Instructions and those purposes detailed herein).

3. Processing Purpose and Instructions

a. The duration of the processing under the Agreement is determined by the parties, as set forth in the Agreement.
b. Company shall process Personal Data only to deliver the Services in accordance with Customer's written Processing Instructions (unless waived in a written requirement), the Agreement and the Data Protection Legislation. Unless permitted under the Agreement or this Addendum, Company shall not otherwise modify, amend, disclose or permit the disclosure of any Personal Data to any third party unless authorized or directed to do so by Customer.
c. Company will not use Personal Data for any use other than as expressly provided in the Agreement or this Addendum. Processing any Personal Data outside the scope

of the Agreement will require prior written agreement between Company and Customer by way of written agreement, and will include any additional fees that may be payable by Customer to Company for carrying out such instructions.

d. Notwithstanding the foregoing, Company shall be entitled to use the Personal Data for statistical and financial purposes provided however that any personal attributes shall be removed from such Personal Data or otherwise if such is maintained on an aggregated basis.

4. Reasonable Security and Safeguards

a. Company represents, warrants, and agrees to use Security Measures (i) to protect the availability, confidentiality, and integrity of any Personal Data collected, accessed, used, or transmitted by Company in connection with this Agreement, and (ii) to protect such data from 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 purchased by Customer.
c. Company shall take reasonable steps to ensure the reliability of its staff and any other person acting under its supervision which has access to and processes 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 Legislation, including implementing appropriate technical and organizational measures.

5. Breach Incidents

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

6. Security Assessments and Audits

Company audits its compliance with data protection and information security standards on a regular basis. Such audits are conducted by Company's internal audit team or by third party auditors engaged by Company.
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), at Customer's expense, 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.

7. 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 EU 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. It is hereby clarified however that if no such response is received from Customer within three (3) business days (or otherwise any shorter period as dictated by the relevant law or authority), Company shall be entitled to provide such information.
c. Notwithstanding the foregoing, Company will cooperate with Customer with respect to any action taken by it pursuant to such order, demand or request, including ensuring that confidential treatment will be accorded to such disclosed Personal Data.
d. Upon reasonable notice, Company shall provide reasonable assistance to Customer in:
    i. allowing Data Subjects to exercise their rights under the Data Protection Legislation, including (without limitation) the right of access, right to rectification, restriction of processing, erasure ("right to be forgotten"), data portability, object to the processing, or the right not to be subject to an automated individual decision making;
    ii. ensuring compliance with any notification obligations of Breach Incidents to the supervisory authority and communication obligations to Data Subjects, as required under Data Protection Legislation;
    iii. Ensuring Customer's 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.

8. Use of Sub-Processors

Customer provides a general consent to Company to engage onward Sub-Processors, provided that Company has entered into an agreement with the Sub-Processor containing data protection obligations that are at least as restrictive as the obligations under this Addendum (to the extent applicable to the services provided by the Sub-processor).
Company will be responsible for any acts, errors or omissions by its Sub-Processors, that may cause Company to breach any of its obligations under this Addendum.

9. Transfer of EEA resident Personal Data outside the EEA

a. Company may transfer and process Personal Data of residents of the EEA or Switzerland outside the EEA ("**Transfer**"), only subject to the following:
    I. The Transfer is necessary for the purpose of Company carrying out its obligations under the Agreement;

    And

    II. One (or more) of the following applies:
        1. The Transfer is done to an Approved Jurisdiction;
        2. The Transfer is done subject to appropriate safeguards (for example, the Privacy Shield as referred to in the COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, or other applicable frameworks);
        3. The Transfer is done in accordance with any of the exceptions listed in the Data Protection Legislation. Customer will inform Company which exception applies to each Transfer and will assume complete and sole liability to ensure that the exception applies.

10. Data Retention and Destruction
    a. Company will only retain Personal Data for as long as Services are provided to Customer in accordance with this 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 by applicable law to retain some or all of 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.
    b. Notwithstanding the foregoing, Company shall be entitled to maintain Personal Data following the termination of this Agreement for statistical and/or financial purposes provided always that Company maintains such Personal Data on an aggregated basis or otherwise after having removed all personally identifiable attributes from such Personal data.

11. 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 modify the terms of this Addendum in circumstances such as (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with Data Protection Legislation, or (iii) to implement or adhere to standard contractual clauses, approved codes of conduct or

certifications, binding corporate rules, or other compliance mechanisms, which may be permitted under Data Protection Legislation. Company will provide notice of such changes to Customer, and the modified Addendum will become effective, in accordance with the terms of the Agreement.

Accepted by _____ (Customer)	**Accepted by** Coralogix **(Company)**.
Authorized Signature:	Authorized Signature: Ariel Assaraf
Print Name	Print Name Ariel Assaraf
Title:	Title: CEO
Date:	Date: 22/01/2018

EXHIBIT A – DATA SHARING PROTOCOL

The personal data transferred concern the following categories of data subjects:
□ Company's end users
□ Company's employees
□ Affiliates and partners

The transfer is made for the following purposes:
□ Log analytics, technical support and improving offerings
□ Consulting, professional, security, storage, hosting and other related services

The personal data transferred may concern the following categories of data:
□ Profile data (name, age, gender, physical address, telephone number, email address)
□ Financial and payment data (e.g. credit card number, transactions)
□ Governmental IDs (passport copy or driver's license)
□ Other: [complete]