Data Processing Agreement

This Data Processing Agreement ("Agreement") forms part of the Contract for Services under the Report URI Terms of Service (the "Principal Agreement").

This Agreement is an amendment to the Principal Agreement and is effective upon its incorporation to the Principal Agreement, which incorporation may be specified in the Principal Agreement or an executed amendment to the Principal Agreement.

Upon its incorporation into the Principal Agreement, this Agreement will form a part of the Principal Agreement.

We periodically update this Agreement. If you have an active Report URI account, you will be informed of any modification by email.

The term of this Agreement shall follow the term of the Principal Agreement.

Terms not defined herein shall have the meaning as set forth in the Principal Agreement. WHEREAS

(A) Your company acts as a Data Controller (the "Controller").

(B) Your company wishes to subcontract certain Services (as defined below), which imply the processing of personal data, to Report URI Ltd., acting as a Data Processor (the "Processor")

(C) The Parties seek to implement a data processing agreement that complies with the requirements of 2018 Data Protection Act, the applied GDPR, and with 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, and repealing Directive 95/46/EC (General Data Protection Regulation -- GDPR).

(D) The Parties wish to lay down their rights and obligations. IT IS AGREED AS FOLLOWS:

1 Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this DPA shall have the following meaning:

1.2 "Company Personal Data" means any Personal Data Processed by a Contracted Processor on Controller's behalf pursuant to or in connection with the Principal Agreement;

1.3 "Contracted Processor" means a Subprocessor;

1.4 "Data Protection Laws" means Data Protection Act 2018, the applied GDPR, and the GDPR;

1.5 "EEA" means the European Economic Area;

1.6 "GDPR" means EU General Data Protection Regulation 2016/679;

1.7 "Data Transfer" means:

1.7.1 a transfer of Company Personal Data from Controller to a Contracted Processor; or

1.7.2 an onward transfer of Company Personal Data from a Contracted Processor to a Subcontracted Processor, or between two establishments of a Contracted Processor,

1.7.3 in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.8 "Services" means report collection services provided by Report-URI. The Service is described more in detail in Schedule 1.

1.9 "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of Controller in connection with the Agreement.

1.10 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2 Processing of Company Personal Data

2.1 Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and

2.1.2 not process Company Personal Data other than on Controller's documented instructions except where required to by UK law. Where such processing is required, Processor shall notify Controller if UK law permits such notification.

2.2 Controller instructs Processor to process Company Personal Data to provide the Services and related technical support.

3 Processor Personnel

3.1 Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4 Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5 Subprocessing

5.1 Processor makes use of multiple required Subprocessors as detailed in the Privacy Policy. On incorporation of this amendment into the Principal Agreement, Controller agrees to the use of these Subprocessors. Controller will be notified 60 days in advance of Processor's intention to appoint new Subprocessors and may terminate their account if they do not agree with the use of such Subprocessors.

6 Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall assist Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Controller obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under the Data Protection Laws. Controller is responsible for determining that the standard reports provided by the Service allow the Controller to fulfil its obligations.

6.2 Processor shall:

6.2.1 promptly notify Controller if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Controller or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform Controller of that legal requirement before the Contracted Processor responds to the request.

7 Personal Data Breach

7.1 Processor shall notify Controller without undue delay upon Processor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Controller with sufficient information to allow Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall co-operate with Controller and take reasonable commercial steps as are directed by Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8 Data Protection Impact Assessment and Prior Consultation

8.1 Processor shall provide reasonable assistance to Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9 Deletion or return of Company Personal Data

9.1 Subject to this section 9 Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the Processing of Company Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data. This is an irreversible step and will occur automatically when Controller terminates the account.

9.2 Processor shall provide on request written certification to Controller that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10 Audit rights

10.1 Subject to this section 10, Processor shall make available to Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by Controller or an auditor mandated by Controller in relation to the Processing of the Company Personal Data by the Contracted Processors. Reasonable fees for the provision of such assistance will be charged by the Processor.

10.2 Information and audit rights of Controller only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11 Data Transfer

11.1 Other than as detailed in the Privacy Policy effective on incorporation of this Amendment to the Principal Agreement, the Processor may not transfer or authorize the transfer of Data to countries outside the UK and/or the European Economic Area (EEA) without prior notification to the Controller. If personal data processed under this Agreement is transferred from a country within the UK or European Economic Area to a country outside the UK or European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12 General Terms

2.1 Confidentiality. Each Party must keep any information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

12.1.1 disclosure is required by law;

12.1.2 the relevant information is already in the public domain.

12.2 Notices. All notices and communications given under this Agreement must be in writing and will be sent by email. Controller shall be notified by email sent to the address related to its use of the Service under the Principal Agreement. Processor shall be notified by email sent to the address: dpa@report-uri.com

13 Governing Law and Jurisdiction

13.1 This Agreement is governed by English law.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of England.

Schedule 1: Service Description and Pricing

The Service offered by Report URI Ltd. is Report URI ("Report URI"). Report URI offers a leading service in the collection and inspection of browser-based telemetry. Report URI provides a complete platform of server-side software and depends on native browser functionality for client-side instrumentation. By utilising Report URI, clients can monitor for performance, security and usability concerns on their website and upon detecting them, work to resolve them.

Report URI provides the ability to collect a user defined amount of reports for an unlimited number of websites.

Schedule 2: Data Processing and Security Description of the data processing carried out on behalf of the Controller

In addition to the information provided elsewhere in the Agreement, the Parties wish to document the following information in relation to the data processing activities. The data processing performed by the Data Processor on behalf of the Controller relates to the service of browser report collection. The data processing details and procedure can be found in the Company's Privacy Policy at https://report-uri.com/home/privacy_policy and the Report URI and Data Protection document at https://cdn.report-uri.com/pdf/Report URI - Data Protection (0v4).pdf.