Data Processing Agreement

PARTIES

This Data Processing Agreement is concluded between ContentKing B.V., having its address at Donauweg 10, 1043 AJ in Amsterdam, The Netherlands, registered with the Chamber of Commerce under registration number 63333996 (hereinafter referred to as “Processor”), and the the (legal) person that is using the Service and that has created an Account for the use of the Service as defined in the Terms of Use (hereinafter referred to as “Controller”. **whereas**

A. The Controller and the Processor concluded an agreement regarding (the use of) the service of Processor, which is used to assess the information about the content of a website being monitored by Controller and its performance, such as metrics concerning its ability to be findable, shareable and optimized for conversions, as well as the API Services (the “Agreement”), of which this Data Processing Agreement forms an integral part;

B. This Data Processing Agreement only applies to the extent the above mentioned services include the processing of personal data, because the website being monitored by Controller includes personal data.

C. Where the processing of personal data is concerned, the Controller qualifies as a data controller and Processor as a data processor under Applicable Law.

D. In this Data Processing Agreement, the Parties set out their arrangements w1ith respect to the processing of personal data in the context of performing the Agreement in accordance with the Applicable Law.

AND HAVE AGREED AS FOLLOWS

Article 1. Definitions

1. This Data Processing Agreement uses the same definitions as those used as in the body of the Agreement and in the Applicable Law, more specifically the General Data Protection Regulation (the "GDPR"), supplemented by the definitions as set out in this Data Processing Agreement.

Applicable Law	the applicable laws and regulations on the processing of personal data including the GDPR and any applicable GDPR implementation act or other national legislation in place in the country of registration of the Controller, as well as any guidelines, policy rules, instructions or recommendations of any government body in respect of the processing of personal data.
Agreement	the agreement concluded between the Controller and the Processor, including the Terms of Use and any addendums and other appendices.
Data Breach	breach relating to personal data as referred to in the Applicable Law.
Data Processing Agreement	this agreement, including recitals and Exhibits, as well as addendums and other appendices, forming an integral part of the Agreement.
Exhibit	appendix to this Data Processing Agreement.
GDPR	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).

Article 2. Subject of this Data Processing Agreement

1. This Data Processing Agreement relates to the processing of personal data by Processor on behalf of Controller as part of the performance of the Agreement. An overview of the categories of personal data, categories of data subjects, the engaged sub-processors, the retention periods and the purposes of processing, is included in Exhibit A.

2. This Data Processing Agreement constitutes an inseparable part of the Agreement. In the event that the provisions of the Data Processing Agreement are inconsistent with the provisions of the Agreement, the provisions of the Data Processing Agreement shall prevail.

Article 3. Data Processing Activities

1. Processor shall only process personal data on behalf of the Controller if the Controller has provided specific written instructions to that effect in Exhibit A of this Data Processing Agreement.

2. Processor will not use the personal data which it processes in the context of this Data Processing Agreement for its own or third-party purposes without Controller's express written consent, unless a legal provision under Applicable Law requires Processor to do so. In such case, Processor shall immediately inform Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3. Controller is responsible and liable for the processing of personal data in relation to the Agreement and guarantees that the instructed processing is in compliance with the Applicable Law. Controller will indemnify and hold Processor harmless against any and all claims of third parties, those of the relevant supervisory bodies and data subjects in particular, resulting in any way from not complying with this guarantee.

4. In case that Processor is of the opinion that an instruction relating to the provisions of this paragraph infringes the Applicable Law, Processor will inform Controller without undue delay via the email address known. Once informed that one of its instructions may be in breach of the Applicable Law, Controller will assess the situation and determine whether the instruction actually violates the Applicable Law. If Controller persists with the unlawful instruction or does not respond adequately, Processor is entitled to terminate the Data Processing Agreement and the Agreement without becoming liable for the consequences thereof.

5. Controller acknowledges that Processor is a Dutch company that complies with Dutch (data protection) regulations. Controller shall stipulate to Processor in writing all local regulatory requirements which apply to the processing of the personal data in its jurisdiction.

Article 4. Technical and Organizational Provisions

1. Processor will, taking into account the nature of the processing and insofar as this is reasonable possible, assist Controller in ensuring compliance with the obligations pursuant to the Applicable Law to take appropriate technical and organizational measures to ensure a level of security appropriate to the risks of the data processing activities. These measures will guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, in view of the risks entailed by the data processing activity and the nature of the data to be protected.

2. Processor will attach a description of the main appropriate technical and organizational measures to be taken by Processor in Exhibit B, which include in any case:
    a. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    b. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    c. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

3. The Parties acknowledge that security measures are subject to change. Processor will endeavour to audit and evaluate, or give instructions to audit and evaluate, the security measures and will promptly modify them to the extent necessary. Where it concerns the main features of the security measures, Processor will inform the Controller in a timely manner of any (intended) changes. Controller may object to these changes in writing within seven days of being notified of the changes by Processor. If agreeing with Controller's objections adversely affects the continuity or the quality of the services to be provided, the Parties will consult. If Controller does not object within seven days, this will be interpreted as an authorization.

Article 5. Confidentiality

1. Employees, subcontractors and other persons involved by Processor and working under the guidance and supervision of Processor, have only access to the personal data to the extent necessary in order to perform the agreed services under the Agreement. Processor will ensure that these persons or parties maintain the same level of confidentiality and security as that which it is obliged to maintain, either via a specific contractual agreement or due to statutory obligations already in place.

Article 6. Sub-processors and Transfers Outside the EEA

1. Controller consents to Processor engaging the third parties ("sub-processors") to carry out the processing operations based on this Data Processing Agreement as described in Exhibit A.

2. Processor will inform Controller in a timely manner of any (intended) changes or additions with regard to the engagement of sub-processors. Controller may object to these changes in writing within seven days of being notified of the changes by Processor. If agreeing with Controller's objections adversely affects the continuity or the quality of the services to be provided, the Parties will consult. If Controller does not object within seven days, this will be interpreted as an authorization.

3. Processor will ensure that the sub-processors that it hires observe similar obligations as those it is bound by as a data processor under this Data Processing Agreement. Processor is responsible for the consequences of engaging a sub-processor.

4. Processor will only be permitted to transfer personal data outside the EEA if this is done in compliance with the Applicable Law by entering into the Standard Contractual Clauses as approved by the European Commission in accordance with Article 46(2) GDPR.

Article 7. Liability

1. With regard to the liability and indemnification obligations of Processor under this Data Processing Agreement the stipulation in the Agreement regarding the limitation of liability applies.

2. Without prejudice to article 7.1 of this Data Processing Agreement, Processor is solely liable for damages suffered by Controller and/or third party claims as a result of any processing, in the event the specific obligations of processor under the Applicable Law are not complied with or in case Processor acted in violence of legitimate instructions of Controller.

Article 8. Data Breach

1. If a Data Breach / suspicion of a Data Breach occurs or has occurred, Processor will i) inform Controller without unreasonable delay as soon as it becomes aware of it via the email address known to Processor and ii) take all reasonable measures to prevent or limit (further) violation of the Applicable Law.

2. Processor will, insofar as reasonable, provide all reasonable cooperation requested by Controller in order for Controller to comply with its legal obligations relating to the Data Breach, including:
    a. The (probable) date on which the breach was discovered and/or occurred;
    b. The nature, possible/probable cause and impact of the breach, whether personal data are/were coded, encrypted or rendered incomprehensible or inaccessible in any way;
    c. The categories of data subjects and personal data concerned and, approximately, the number of data subjects and personal data concerned;
    d. The name and contact information of the data protection officer or other person from whom information on the Data Breach may be obtained;
    e. The probable consequences of the breach; and
    f. The measures Processor has proposed or taken or will take to remediate the breach relating to personal data, including, as may be appropriate, measures to limit any adverse consequences of the Data Breach.

3. Reporting a Data Breach to the relevant supervisory body or bodies and/or the data subjects is and will remain at all times the responsibility of Controller. Processor will provide, on request and at Controller's expense, all reasonable cooperation in case of any investigation initiated by the Controller as a result of a Data Breach, of appropriate subsequent steps with regard to the Data Breach, and/or will provide information to the relevant supervisory body or bodies and/or to the data subjects.

Article 9. Cooperation

1. Processor will, insofar as reasonably possible, provide all reasonable cooperation to Controller in order to enable Controller to promptly fulfil its obligations when a data subject exercises his rights based on the Applicable Law, in particular the right of access, rectification, erasure, restriction, data portability and the right to object. Processor will furthermore assist Controller, insofar as reasonably possible, where necessary and upon request, carrying out data protection impact assessments and consultation with relevant supervisory bodies.

2. If Processor receives a request from a data subject that relates to the processing operations for which the Controller qualifies as the data controller, Processor will forward this request to the Controller without unreasonable delay.

3. Processor is entitled to charge any costs associated with the cooperation with Controller as described in this Article.

Article 10. Audit

1. At Controller's request, Processor will make the information available that is required to demonstrate that Processor has complied with the obligations incumbent upon it as a data processor under this Data Processing Agreement, for example by providing the relevant part of its record of data processing activities.

2. Controller may have Processor's processing activities and processing operations audited up to once per year (the "Audit"), with due observance of a prior four-week notice period and taken the following into account:
    a. The Audit's primary purpose is to investigate the technical and organizational security measures and compliance with this Data Processing Agreement and the Applicable Law.
    b. The Audit will be performed by an independent, reputed auditor. Controller will ensure that the auditor is obliged to keep his findings confidential from third parties.
    c. The Audit will be conducted in consultation with Processor at a time and date impede the Processor's business operations as little as possible.
    d. Controller will pay all the costs, fees and expenses related to the Audit, including the internal costs incurred by Processor.

3. The findings of the Audit will be discussed by the Parties and evaluated in consultation, and they will determine in consultation which measures must be taken, if any.

Article 11. Termination

1. With regard to the termination under this Processor's Agreement the specific provisions of the Agreement apply. Without prejudice to the specific provisions of the Agreement, the Processor will, at the first request of the Controller, delete or return all the Personal Data, and delete all existing copies, unless the Processor is legally required to store (part of) the Personal Data. If the return, destruction or removal is not possible, Processor will inform the Controller. In that case, Parties consult for a solution and until that moment, Processor will treat the personal data confidentiality and will refrain from processing them any further.

2. The obligations laid down in this Data Processing Agreement which, by their nature, are designed to continue after termination will also remain in force after the termination of this Data Processing Agreement. If one of the Parties is aware of any such legal requirement, it will inform the other Party as soon as possible.

Article 12. Miscellaneous

1. This Data Processing Agreement replaces any previous arrangements made by the Parties regarding the processing of personal data for the purpose of performing the Agreement.

2. The Processor may implement changes to the processing operations in Exhibit A and Exhibit B as the circumstances may require from time to time. Controller may object to these changes in writing within seven days of being notified of the changes by Processor.

3. If any provision of this Data Processing Agreement proves not to be valid or not enforceable, this invalidity or unenforceability will not affect the validity and enforceability of the other provisions in this Data Processing Agreement. If a provision is not valid or not enforceable, the Parties will endeavour as soon as possible in reasonableness and fairness to agree a replacing provision that is valid and enforceable and that, to the extent possible, has the same meaning and content as the provision it replaces.

This Data Processing Agreement is governed by the law that applies to the Agreement. Any and all disputes arising from or in connection with this Data Processing Agreement will be submitted to the court that is designated as the competent court in the Agreement.

EXHIBIT A

Description of the data processing activities.

1. **SUBJECT-MATTER, NATURE AND PURPOSE OF THE PROCESSING:**
   The context and purpose for the Processing of the Personal Data is the Processor's provision of the applicable Services to Controller, which is used by Controller to assess the Content Information of a Controller Website, as further specified in the Terms of Use, as well as the API Services.

2. **DURATION OF PROCESSING:**
   Processing of the Personal Data by Processor shall be for the term of the Agreement.

3. **CATEGORIES OF PERSONAL DATA:**
   The information about the content of a website being monitored by Controller and its performance, such as metrics concerning its ability to be findable, shareable and optimized for conversions. Processor will Process Personal Data as far as the aforementioned website contains any Personal Data.

4. **CATEGORIES OF DATA SUBJECTS**
   Data subjects whose Personal Data are included on the website being monitored by Controller using the Services provided by Processor.

5. **SUB-PROCESSORS**
   Name:
   ContentKing Global Infrastructure B.V.
   Address:
   Meidoornkade 22, 3992 AE, Houten, NL
   Contact person's name, position and contact details:
   Marek Le Xuan, DPO, dpo@contentkingapp.com
   Description of processing:
   Hosting, customer support and sales & marketing operations.

   Name:
   ContentKing Czech Republic s.r.o.
   Address:
   Masarykova 412/32, Brno-město, 602 00 Brno, CZ
   Contact person's name, position and contact details:
   Marek Le Xuan, DPO, dpo@contentkingapp.com
   Description of processing:
   Customer support, product development and sales & marketing operations.

EXHIBIT B

Description of the technical and organisational measures taken by Processor.

1. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
2. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
3. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing
4. Measures for user identification and authorization
5. Measures for the protection of data during transmission
6. Measures for the protection of data during storage
7. Measures for ensuring physical security of locations at which personal data are processed
8. Measures for ensuring events logging
9. Measures for ensuring system configuration, including default configuration
10. Measures for internal IT and IT security governance and management
11. Measures for certification/assurance of processes and products
12. Measures for ensuring data quality
13. Measures for ensuring accountability
14. Measures for allowing data portability and ensuring erasure