Wheel Of PopUps

If a signed **Data Processor Agreement** is required by your legal team, please follow these steps:

Please fill out the following form and send a signed scan to **support@wheelofpopups.com** and your account manager will reply with a signed copy.

DATA PROCESSOR AGREEMENT

This Data Processor Agreement is entered into force on _________________.

between

____

____

____

____

(*"the Controller"*)

and

Earn Coupon doo Belgrade
ID 20904453, Vodovodska 75, Suite 5
11030 Belgrade
Serbia
(*"the Processor"*)

(collectively *"the Parties")*

1. BACKGROUND AND PURPOSE

1.1 The Controller has subscribed to services under the Processor's subscription terms and conditions (the "Main Agreement"), and the Processor delivers a promotion building service to the Controller by providing lead capture forms (*"Wheel of Popups"*). When providing these services to the Controller, the Processor processes personal data for which the Controller is responsible, thus the Processor processes personal data on behalf of the Controller.

1.2 This Agreement constitutes an appendix to the Main Agreement entered into between the Parties. In the event of conflicts between the agreements, this Agreement shall take precedence.

1.3 The Parties have entered into this Data Processor Agreement (*"Agreement"*) in order to fulfil the requirement of a written agreement between a data controller and a data pro- cessor of personal data as set out in section 28(3) of the EU General Data Protection Regulation 2016/679 (*the "GDPR"*).

2. SCOPE

2.1 The scope of this Agreement is to govern the relationship between the Controller and the Processor.

2.2 This Agreement is aimed at the Data Controller as well as the Data Processor, and the fundamental basis for this Agreement is the fact that completion of data processing by a data processor must take place in accordance with an agreement between the Parties.

3. PROCESSING OF DATA

3.1 The Processor may only process personal data under the instructions of the Controller. The Controller's instructions at the time of entry into this Agreement is set forth in Appendix 1, thus the Processor may only process the categories of personal data and data regarding the data subjects as listed in Appendix 1.

3.2 The Controller is responsible for obtaining the data subject's consent to the processing of data in question in accordance with article 7 and article 8 of the GDPR.

3.3 The Processor is not entitled to process the Controller's personal data for any other purposes than the ones set forth in Appendix 1, as amended from time to time, unless the Controller has given prior written consent to the processing in question.

3.4 Upon a written request from the Controller, the Processor must correct, block or delete personal data, which is incorrect or incomplete.

3.5 Upon a written request from the Controller, the Processor must present the necessary documentation proving that the processing of personal data is carried out in accordance with the applicable data protection laws and the GDPR, thus the Processor must keep records of its processing activities.

3.6 The Processor must assist the Controller in fulfilling its legal obligations under GDPR chapter 3 concerning the rights of the data subject. If the Processor receives a request from a data subject for access to the data subject's registered personal data, or a data subject objects to the processing of his or her personal data, the Processor must inform the Controller of the request or objection without undue delay.

3.7 The Processor must delete personal data, copies and records thereof when it is no longer reasonably necessary to perform the Processor's obligations under the Main Agreement. In any case the Processor deletes the personal data collected on behalf of the Controller when the data has been stored with the Processor for 12 months. If the Controller wishes for the Processor to keep processing the data past these 12 months, it rests with the Controller to provide the Processor with the necessary documentation proving a substantiated purpose for extended processing.

4. USE OF SUB PROCESSORS

4.1 The Processor may only use sub processors when this is authorized by the Controller.

4.2 By signing this Agreement, the Controller authorizes the Processor to use the sub processors listed in Appendix 1.

4.3 Before the Processor engages a new sub processor, the Processor shall notify the Controller thereof and provide information about the new sub processor's name and location for processing. If the Controller has a reasonable basis to object to the Processor's use of a new sub processor and therefore wishes to terminate this Agreement and the Main Agreement, the Controller shall notify the Processor within 10 business days after receipt of the Processor's notice.

4.4 The Processor ensures that any sub processor engaged by the Processor to carry out specific processing activities on behalf of the Controller, is bound by data protection obligations no less stringent than the ones set forth in this Agreement. If the sub processor fails to fulfil its data protection obligations, the Processor is liable to the Controller for the performance of the sub processor's obligations.

4.5 Upon the Controller’s request, the Processor must provide the Controller with sufficient information to ensure the Controller that the sub processors engaged by the Processor have taken the necessary technical and organizational security measures.

5. CONFIDENTIALITY

5.1 All employees employed by the Processors receive appropriate training, adequate instructions and guidelines for processing personal data.

5.2 The Processor must limit access to personal data to the relevant employees and ensure that these are authorized to process the personal data.

5.3 The Processor must ensure that the employees of the Processor, who process personal data, are bound by adequate confidentiality obligations. Such obligations shall survive the termination of this Agreement.

6. AUDITS

6.1 The Controller is entitled to, at its own cost, take proportionate and commercially reasonable measures to validate the Processor’s compliance with this Agreement, either by itself or by using a third party to conduct the audit.

6.2 If the Controller takes on a third party to conduct the audit on behalf of the Controller, the Controller must ensure that the third party carrying out the audit enters into a nondisclosure agreement and that such third party takes necessary security measures when conducting the audit.

6.3 Audits must be conducted during the Processor’s business hours and the Processor must be notified of planned audits within reasonable time prior to the audit. The audit shall not grant the Controller access to the Processor’s trade secrets or proprietary information unless this is required in order for the Controller to comply with the applicable data protection law.

7. DATA TRANSFER

7.1 The Processor is not entitled to transfer or hand over data to third parties or sub processors without prior written instruction hereto from the Controller, unless such transfer or handing over is provided by law.

7.2 The Controller hereby consents to the transfer of EU Personal Data to, and the processing of EU Personal Data in, the United States of America and Serbia. The parties hereby enter into the Standard Contractual Clauses for Processors, as approved by the European Commission under Decision 2010/87/EU, attached hereto as Exhibit C (the “SCCs”) and made a part of this DPA in their entirety.

8. SECURITY MEASURES

8.1 The Processor must take the necessary technical and organizational security measures to ensure a level of security in accordance with the GDPR and appropriate to the risk presented to the processing and the nature of the personal data to be protected, having regard to the state of the art and the cost of their implementation. The measures shall take into account the requirements set out in article 32 of the GDPR and include but not be limited to

8.1.1 safeguarding personal data against being destroyed accidentally or illegally, lost, altered, damaged or made known to unauthorized persons, misused or in any other way illegally processed,

8.1.2 taking measures to prevent transfers to any unauthorized person or entity,

8.1.3 ensuring that records are maintained of access to personal data, and

8.1.4 taking measures to ensure personal data remains available.

8.2 Security measures taken by the Processor are stated in Appendix 2.

8.3 The Processor shall periodically assess data security risks related to the provisioning of the services to the Controller.

8.4 Upon the Controller’s request, the Processor must provide the Controller with sufficient information to ensure the Controller that the Processor has taken the necessary technical and organizational security measures.

9. BREACH OF DATA SECURITY

9.1 The Processor must notify the Controller of personal data security breaches, operational malfunctions or suspected security breaches relating to the processing of personal data without undue delay and within 24 hours after the security breach has been discovered, unless the Processor is able to demonstrate that the data security breach is unlikely to result in a risk to the rights and freedoms of data subjects.

9.2 The notification in clause 9.1 must (if relevant) contain:

9.2.1 a description of the data security breach including the categories and approximate amount of data and data subjects concerned,

9.2.2 the name and contact details of the Processor’s data protection officer,

9.2.3 a description of the likely consequences of the data security breach,

9.2.4 a description of the measures taken or proposed to be taken by the Controller to address the data security breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where and in so far as it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

9.3 The Processor shall document any data security breaches. The documentation shall only include information necessary for the Controller to verify compliance with the applicable data protection law to the relevant supervisory authority.

9.4 The Controller is responsible for notifying the relevant supervisory authority about the data security breach.

10. LIMITATION OF LIABILITY

10.1 Pursuant to article 82(2) of the GDPR, the Processor shall only be liable for damage caused by processing where the Processor has not complied with obligations of the GDPR specifically directed to processors or where the Processor has acted outside or contrary to this Agreement.

10.2 The Processor shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

10.3 The Processor's cumulative liability to the Controller or any other party for any loss or damages resulting from claims, demands or actions arising out of relating to this Agree- ment shall not exceed the total paid-in fee from the Controller to the Processor within the 12 months previous to the date the claim is first brought against the Processor.

11. INDEMNIFICATION

11.1 If the Controller, against the regulations set forth in Appendix 1, collects sensitive personal data and thus makes the Processor process such information, the Controller undertakes to indemnify and hold the Processor harmless for any and all damages and losses incurred by the Processor due to the Controller's breach of the Agreement.

12. AMENDMENTS

12.1 Any amendments to this Agreement must be in writing and signed by the Parties in order to be binding.

13. TERM AND TERMINATION

13.1 This Agreement shall enter into force on the date of signing and shall remain in force for as long as the Processor processes personal data on behalf of the Controller.

13.2 Upon termination of the Main Agreement, this Agreement will be terminated accordingly.

13.3 If one of the Parties is in breach of this Agreement, the other Party shall be entitled to terminate this Agreement with a written notice of 10 business days. If the Party in breach has not remedied the breach within 10 business days, the Party not in breach is entitled to terminate the Agreement on the date stated in the 10 day-notice.

13.4 Upon termination of this Agreement, the Controller must notify the Processor to delete or return the personal data. The Processor is obliged to destroy or return the personal data as requested, unless legislation imposed upon the Processor prevents it from destroying or returning all or parts of the personal data. The Controller must allow for a period of 30 days in order for the Processor to complete the full deletion of personal data.

14. GOVERNING LAW AND DISPUTES

14.1 Any disputes arising from this Agreement must be resolved and governed as agreed in section 16 of the Main Agreement, the only amendment being that this Agreement is governed by the GDPR in addition to laws of the State of New York.

15. SIGNATURES AND COPIES

15.1 This Agreement is issued in two original copies with each Party is handed one original copy.

Date: ____________________

On behalf of the Controller:

____

____

Date: ____________________

On behalf of the Processor:

Rade Joksimovic
Director, Earn Coupon doo

APPENDIX 1

This appendix constitutes a part of the Agreement and must be filled out by the Parties.

DATA SUBJECTS

The personal data processed by the Processor on behalf of the Controller concerns the following categories of data subjects:

[Visitors of the Controller’s website, who have registered their data in the spaces selected by the Controller in a given Wheel of Popups promotion.]

CATEGORIES OF PERSONAL DATA

The Processor processes the following categories of personal data on behalf of the Controller:

[e-mail addresses, first and last names, other contact information, age, date of birth, gender, technical details (including IP-address), behavior details (including URLs visited, events triggered on defined actions such as page loads, clicks, log-ins, time spent on page or site), geo-location data (aggregated estimate based on collected IP-address) and Wheel of Popups’ specific events (contact details submitted, redirection to other pages or sites, Wheel of Popups promotions shown/closed).]

PROCESSING ACTIVITIES

The following processing activities will be carried out by the Processor on behalf of the Controller:

[Collection of data on the Controller’s websites either via direct submissions from visitors on the Controller’s websites or from behavioral analytics tracking the Controller’s website, systematization and analysis of data and storing of data via sub processors and thus transferring data to sub processors. Data will be accessed by the Processor for the purpose of maintenance, global analytics or support to the Controller. Upon instruction from the Controller, the Processor forwards the Controller’s data to third parties appointed by the Controller.]

PRE-APPROVED SUB PROCESSORS

The following sub processors used by the Processor are pre-approved by the Controller:

Entity name and address	**Entity type**	**Entity Country**
[Amazon Web Services]	[Hosting provider]	[Luxembourg, USA]
[Paddle]	[Payment processor]	[UK]
[Laravel]	[Server management]	[USA]
[Zapier]	[Data integration]	[USA]

PROCESSING LOCATION

The processing of personal data by the Processor on behalf of the Controller will take place in the following location:

For the Processor:	[Serbia]
For the pre-approved sub processors:	[Luxembourg, USA, UK]

APPENDIX 2

This appendix constitutes a part of the Agreement and must be filled out by the Parties.

The Parties have agreed to the following security measures to be taken in connection with the Processors processing of personal data on behalf of the Controller:

PHYSICAL ACCESS CONTROL

Measures to prevent physical access of unauthorized persons to IT systems that handle personal data:

[Buildings and systems used for data processing are safe. Data processing media is stored properly and is not available to unauthorized third parties, thus such media is kept locked when unattended. The Processor only uses high-quality hardware and software and continues to update these if relevant.]

SYSTEM ACCESS CONTROL

Measures to prevent unauthorized persons from using IT systems:

[The Processor maintains an authentication system for accessing personal data processing systems. Employee accounts are not shared and inactive sessions are terminated after 30 minutes. The Processor keeps network logs and a log of detection of intrusion.]

DATA ACCESS CONTROL

Measures to ensure that the Processors employees only have access to the personal data pursuant to their access rights:

[The access to personal data is role based. Data can only be accessed by the Processor or the Controller. Access to databases are IP restricted. The Processor has also introduced log-in and password procedures ensuring that only employees with access rights have access to personal data. The Processor keeps a list of employees that have access to the Controller's data, and only key employees have access to databases.]

TRANSMISSION ACCESS CONTROL

Measures to ensure that personal data cannot be read, copied, altered or deleted by unauthorized persons during electronic transmission or during transport or storage on data media and that those areas can be controlled and identified where transmission of personal data is to be done via transmission systems:

[All data submitted by the Controller is transferred to the Processor encrypted, if the Controller's website is running on a secure HTTPS connection. All data is encrypted on storage.]

ENTRY CONTROL AND TRACEABILITY

Measures to ensure that it can be subsequently reviewed and determined if and from whom personal data was entered, altered or deleted in the IT systems, as well as measures to ensure the accountability and traceability of the processing of personal data:

[The Processors applies a log monitoring solution to collect and compare logged events. The Processor keeps network logs and a log of detection of intrusion. All services provided by the Processors are thus being logged and stored for 15-30 days. The logs contain information on who accessed data, from which IP address the data was accessed, which data were accessed and when data was accessed. The Processor performs internal audits to ensure that all security measures stated in this Appendix are taken and that each new feature or amendment to services provided by the Processor live up to these standards.]

AVAILABILITY CONTROL

Measures to ensure that personal data is protected against accidental destruction or loss:

[The Processor has set up and maintained web application firewall and anti-virus software as well as back-up procedures as layers of security. The service provided by the Processor runs on a combination of serverless and CDN. The CDN is the Amazon Web Services S3, which runs at the capacity of 40 Gbps and a 100.000 requests per second. The service provided by the Processor runs in an Amazon Web Services Lambda environment, enabling scale on demand. The Processor maintains recovery processes to allow for continuation of data processing and to provide an effective and accurate recovery of personal data.]

TRANSPARENCY

Measures to provide a description of any procedures established to ensure an adequate level of transparency to the Controller regarding the Processor and sub processors processing of personal data:

[The Controller will be able to access data submitted by the Processor for as long as the Controller has an active paid subscription plan with the Processor, during which time all Analytics and Leads data will be viewable in the Wheel of Popups dashboard provided by the Processor.]

INTERVENEABILITY

Measures to ensure that the Controller is allowed to access, rectify, delete, block and manage objections to the processing of personal data:

[The Controller is able to download data submitted by visitors on the Controller’s website in CSV format through the Wheel of Popups Dashboard provided by the Processor for as long as the Controller has an active paid subscription with the Processor. If the Controller wishes to rectify, delete or block data or in any other way wishes to manage objections to the processing of personal data, the Processor must notify the Processor of such wishes by contacting the Wheel of Popups Customer Success Team. The Wheel of Popups Customer Success Team will validate the ownership of data and perform the requested actions. The Processor does not enable editing of personal data. Incorrect personal data will thus be deleted and must be resubmitted in its correct form by the data subject.]

PORTABILITY

Measures to ensure the portability of personal data, if the migration of data is requested by the Controller or data subjects:

[Data submitted by the data subjects (visitors on the Controller’s websites) will be downloadable through the Wheel of Popups Dashboard provided by the Processor.]

DATA RETENTION AND DELETION

Measures to ensure that personal data is adequately erased or destroyed when use of the personal data is no longer necessary:

[Personal data is stored for 12 months, after which it is deleted if the Controller has not pleaded clause 3.7 of this Agreement. Data is deleted upon request from the Controller.]

After the termination of the DPA, clause 13.4 of the Agreement applies.