Data Processing Agreement

This Data Processing Agreement ("**DPA**"), forms part of the Agreement between GetWebCraft Limited ("**GetWebCraft**") and ***LIes MAl! - Schülerzeitung der Limesschule Altenstadt*** ("**Customer**") and shall be effective on the date both parties execute this DPA (“**Effective Date**"). All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement.

By signing the DPA, Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of its Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term “Customer” shall include Customer and Customer’s Affiliates.

In the course of providing the Services to Customer pursuant to the Agreement, GetWebCraft may Process Personal Data on behalf of Customer and where GetWebCraft Processes such Personal Data on behalf of Customer the Parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

1. Definitions

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “Control,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“**Authorized Affiliate**” means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between Customer and GetWebCraft.

"**Agreement**" means GetWebCraft’s Terms of Service found at https://getsitecontrol.com/terms/, which govern the provision of the Services to Customer, as such terms may be updated by GetWebCraft from time to time.

"**Customer Data**" means any Personal Data that GetWebCraft processes on behalf of Customer as a Data Processor in the course of providing Services, as more particularly described in this DPA.

"**Data Protection Laws**" means all applicable laws relating to the processing of Personal Data including, while it is in force and applicable to the processing of Personal Data under the Agreement, the General Data Protection Regulation (Regulation (EU) 2016/679)

"**Data Controller**" means an entity that determines the purposes and means of the processing of Personal Data.

“**Data Subject**” means the identified or identifiable person to whom Personal Data relates.

"**Data Processor**" means an entity that processes Personal Data on behalf of a Data Controller.

"**EU Data Protection Law**" means (i) prior to 25 May 2018, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of Personal Data and on the free movement of such data ("**Directive**") and on and after 25 May 2018, 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 (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (as may be amended, superseded or replaced).

"**EEA**" means, for the purposes of this DPA, the European Economic Area, United Kingdom and Switzerland.

"**Personal Data**" means any information relating to an identified or identifiable natural person.

"**Privacy Shield**" means the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Framework self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"**Privacy Shield Principles**" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision C(2016)4176 of 12 July 2016 (as may be amended, superseded or replaced).

"**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. "Process", "processes" and "processed" shall be interpreted accordingly.

"**Security Incident**" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data.

"**Sensitive personal data**" means special categories of personal data and has the meaning given to it in the GDPR.

"**Services**" means any product or service provided by GetWebCraft to Customer pursuant to the Agreement.

"**Sub-processor**" means any Data Processor engaged by GetWebCraft in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

2. Scope and Applicability

2.1 This DPA applies where and only to the extent that GetWebCraft processes Customer Data that originates from the EEA and/or that is otherwise subject to EU Data Protection Law on behalf of Customer as Data Processor in the course of providing Services pursuant to the Agreement.

2.2 If the Customer entity signing this DPA is a party to the Agreement, this DPA is an addendum to and forms part of the Agreement.

2.3 If the Customer entity signing this DPA is not a party to the Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Agreement executes this DPA.

3. Processing of Data

3.1 **Role of the Parties**. As between GetWebCraft and Customer, Customer is the Data Controller of Customer Data, and GetWebCraft shall process Customer Data only as a Data Processor acting on behalf of Customer.

3.2 **Customer Processing of Customer Data**. Customer agrees that (i) it shall comply with its obligations as a Data Controller under Data Protection Laws in respect of its processing of Customer Data and any processing instructions it issues to GetWebCraft; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for GetWebCraft to process Customer Data and provide the Services pursuant to the Agreement and this DPA.

3.3 **GetWebCraft Processing of Customer Data**. The Processor may only process Personal Data under the instructions of the Controller. The Controller’s instructions at the time of entry into this DPA is set forth in Appendix 1, thus the Processor may only process the categories of Personal Data as listed in Appendix 1. The Processor is not entitled to process the Controller’s Personal Data for any other purposes than the ones set forth in Appendix 1 unless Controller has given prior written consent to the processing in question.

3.4 Upon written request from the Controller, the Processor must correct, block or delete Personal Data which is incorrect or incomplete.

3.5 The Processor must assist the Controller in fulfilling its legal obligations under GDPR concerning the rights of the Data Subject. If the Processor receives a request from a Data Subject for access to the Data Subject’s 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.

3.6 **Details of Data Processing**

(a) Subject matter: The subject matter of the data processing under this DPA is the Customer Data.

(b) Duration: As between GetWebCraft and Customer, the duration of the data processing under this DPA is until the termination of the Agreement in accordance with its terms.

(c) Purpose: The purpose of the data processing under this DPA is the provision of the Services to the Customer and the performance of GetWebCraft’s obligations under the Agreement (including this DPA) or as otherwise agreed by the parties.

(d) Nature of the processing: GetWebCraft provides website widget services and other related services, as described in the Agreement.

(e) Categories of data subjects: any individual whose information is stored on or collected via the Services.

3.7 Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that GetWebCraft shall have a right to use and disclose data relating to the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered Personal Data under Data Protection Laws, GetWebCraft is the Data Controller of such data and accordingly shall process such data in accordance with the GetWebCraft Privacy Policy and Data Protection Laws.

4. Subprocessing

4.1 **Authorized Sub-processors**. Customer agrees that GetWebCraft may engage Sub-processors to process Customer Data on Customer's behalf. The Sub-processors currently engaged by GetWebCraft and authorized by Customer are listed in Appendix 1. By signing this DPA, the Controller authorizes the Processor to use the Sub-processors listed in Appendix 1. The Processor may only use Sub-processors when this is authorized by the Controller. Any such Sub-processors will be permitted to obtain Personal Data to deliver the services GetWebCraft has retained them to provide for the purpose of the Agreement.

4.2 **Sub-processor Obligations**. GetWebCraft shall remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause GetWebCraft to breach any of its obligations under this DPA.

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 DPA and the Agreement, the Controller shall notify the Processor within 10 business days after receipt of the Processor’s notice.

4.4 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 Processor 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 under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

6. Data Transfer

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

6.2 **Data center locations**. GetWebCraft may transfer and process Customer Data anywhere in the world where GetWebCraft or its Sub-processors maintain data processing operations. GetWebCraft shall at all times provide an adequate level of protection for the Customer Data processed, in accordance with the requirements of Data Protection Laws.

6.3 **Privacy Shield**. To the extent that GetWebCraft processes any Customer Data protected by EU Data Protection Law under the Agreement and/or that originates from the EEA, in a country that has not been designated by the European Commission or Swiss Federal Data Protection Authority (as applicable) as providing an adequate level of protection for Personal Data, the parties acknowledge that GetWebCraft shall be deemed to provide adequate protection (within the meaning of EU Data Protection Law) for any such Customer Data by virtue of compliance with Privacy Shield. GetWebCraft agrees to protect such Personal Data in accordance with the requirements of the Privacy Shield

Principles. If GetWebCraft is unable to comply with this requirement, GetWebCraft shall inform Customer.

7. Security Measures

7.1 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

7.1.1 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,
7.1.2 taking measures to prevent transfers to any unauthorized person or entity,
7.1.3 taking measures to ensure personal data remains available.
7.2 Security measures taken by the Processor are stated in Appendix 2.

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

8. Breach of Data Security

8.1 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.

The notification in clause 8.1 must (if relevant) contain:
8.2.1 a description of the data security breach including the categories and approximate amount of data and data subjects concerned,
8.2.2 a description of the likely consequences of the data security breach,
8.2.3 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.

8.2 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.

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

9. Limitation of Liability

9.1 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 DPA.

9.2 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.

9.3 The Controller agrees that:
(i) An unsuccessful Security Breach attempt will not be subject to this Article. An unsuccessful Security Breach attempt is one that results in no unauthorized access to Controller Personal Data or to any of Processor’s equipment or facilities storing Controller Personal Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and
(ii) Processor’s obligation to report or respond to a Security Breach under this Article is not and will not be construed as an acknowledgement by Processor of any fault or liability with respect to the Security Breach.

10. Indemnification

10.1 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 DPA.

11. Term and Termination

11.1 This DPA 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.

11.2 Upon termination of the Agreement, this DPA will be terminated accordingly.

11.3 If one of the Parties is in breach of this DPA, the other Party shall be entitled to terminate this DPA 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 DPA on the date stated in the 10 day notice.

11.4 Upon termination of this DPA, 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.

12. Return or Deletion of Data

12.1 The Processor must delete all Customer Data in its possession or control, copies and records thereof when it is no longer reasonably necessary to perform the Processor’s obligations under the Agreement. The Processor will retain some or all of the Customer Data if it is instructed by the Customer, if it is required by applicable law or by the authorized body.

13. Cooperation

13.1 The Services provide Customer with a number of controls that Customer may use to retrieve or delete Customer Data, which Customer may use to assist it in connection with its obligations under the GDPR, including its obligations relating to responding to requests from data subjects or applicable data protection authorities. To the extent that Customer is unable to independently access the relevant Customer Data within the Services, GetWebCraft shall provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to GetWebCraft, GetWebCraft shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If GetWebCraft is required to respond to such a request, GetWebCraft shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

13.2 If a law enforcement agency sends GetWebCraft a demand for Customer Data (for example, through a subpoena or court order), GetWebCraft shall attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, GetWebCraft may provide Customer’s basic contact information to the law enforcement agency. If compelled to disclose Customer Data to a law enforcement agency, then GetWebCraft shall give Customer reasonable notice of the demand to allow Customer to seek a protective order or another appropriate remedy unless GetWebCraft is legally prohibited from doing so.

13.3 To the extent GetWebCraft is required under EU Data Protection Law, GetWebCraft shall provide reasonably requested information regarding the Services to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

14. Governing Law and Disputes

14.1 Any disputes arising from this DPA must be resolved and governed as agreed in the Agreement, the only amendment being that this DPA is governed by the GDPR in addition to Cyprus law.

IN WITNESS WHEREOF, the parties have caused this DPA to be executed by their authorized representative:

GetWebCraft Limited

By:

Name: Alexey Umilin

Title: CEO

Date: April 27, 2018

LIes MAl! - Schülerzeitung der Limesschule Altenstadt

Name: Tanja Schäfer-Auth

Title: Chefredakteurin

Date: April 27, 2018

APPENDIX 1

This appendix constitutes a part of the DPA 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 entered their data in the spaces selected by the Controller in a given widget created using the Services.]

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 URL’s visited, events triggered on defined actions such as page loads, clicks, logins, time spent on page or site), geolocation data (aggregated estimate based on collected IP-address) and widget specific events (newsletter sign-up, contact details submitted, redirection to other pages or sites, widgets shown/closed).] The Processor does not process Sensitive Personal Data, thus the Controller may not use the widgets to collect and make the Processor process Sensitive Personal Data. The Controllers collection of sensitive personal data will be construed as a breach of this DPA.

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:

- Amazon Web Services, Inc
- The Rocket Science Group, LLC (Mailchimp)
- Help Scout, Inc

APPENDIX 2

This appendix constitutes a part of the DPA 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 hard- 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.]

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. The Processor has introduced login 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.]

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 dashboard provided by the Processor.]