



Data Processing Agreement

Link-Busters Operations B.V.

[Last version: may 2018]

This Data Processing Agreement, which is GDPR compliant, is a supplement of the Master Services Agreement (hereafter: “MSA”) between Link-Busters Operations B.V., having its registered seat in Amsterdam, and having its registered office at Nachtwachtlaan 20, 1058 EA Amsterdam, registered with the Trade Register (Handelsregister) with number 56543336 (hereafter: “Link-Busters” or “Data Processor”) and our clients (hereafter: “Client” or “Data Controller”) with which we have entered the MSA and who have agreed to this Data Processing Agreement. Capitalized terms used, but not defined, in this DPA are defined in the MSA.

Whereas

- A. The terms used in this Agreement (in particular terms beginning with a capital letter) correspond with the terms used General Data Protection Regulation (GDPR). This Agreement will be interpreted accordingly. The GDPR will hereinafter also be referred to as “**Relevant Privacy Legislation**”.
- B. Data Processor is a company active in the field of online anti-piracy services. See www.link-busters.com for more information. Data Processor provides services to detect and remove unlawful links to copyright protected material to its clients (the “**Services**”).
- C. Data Controller is a Client of Link-Busters. Data Controller wishes to make use of the Services. In this respect, Link-Busters and the Client have entered into a Master Services Agreement, of which this Data Processing Agreement is a supplement.
- D. The use of the Services implies the Processing of Personal Data, which must be carried out in accordance with the Relevant Privacy Legislation.
- E. Link-Busters and Client agree that in respect of the use of the Services and the consequent Processing of Personal Data, Client will act as Data Controller and Link-Busters will act as Data Processor within the meaning of the Relevant Privacy Legislation.
- F. The Relevant Privacy Legislation requires a Data Processing Agreement between Data Controller and Data Processor. Furthermore, the Relevant Privacy Legislation obliges Data Controller to ensure that Data Processor guarantees sufficient safety measures concerning the processing of the Personal Data. Data Controller is obliged to supervise the accomplishment of these safety measures.
- G. Link-Busters and Client hereby enter into such a Data Processing Agreement (the “**Agreement**”) in order to regulate the provision and the use of Personal Data that Data Processor will be processing on behalf of Data Controller. This will not include the data collected by Link-Busters to use for its own purposes, for which data Link-Busters acts as a Data Controller itself. This Agreement regulates Link-Busters’ position as Data Processor in processing the data and content on behalf of Data Controller.

Agreement

1 Obligations of the Data Controller

- 1.1 **Data and information:** Through offering Data Controller the Services, Data Processor receives (Personal) Data. Data Controller shall provide all other information which Data Processor may reasonably require in order for Data Processor to (a) provide the services as agreed on in the MSA and (b) comply with this Agreement.

1.2 **Compliance with law:** The instructions given by Data Controller to Data Processor in respect of the (Personal) Data shall at all times be in accordance with the Relevant Privacy Legislation.

2 **Obligations of the Data Processor**

2.1 **Compliance with law:** Data Processor will comply with the Relevant Privacy Legislation, as far as it concerns obligations that directly apply to Data Processors.

2.2 **Instructions of Data Controller, purpose and means of Processing Personal Data:** Data Processor undertakes that it shall process the Personal Data strictly and only on behalf of Data Controller, in accordance with Data Controller's documented instructions and under Data Controller's responsibility, except in the case the law requires Data Processor otherwise. Data Processor will not process Personal Data for any purpose other than as established by Data Controller. Data Processor has no control over the purposes and means of the processing of Personal Data.

2.3 **Confidentiality:** Data Processor will treat the Personal Data, and any other information provided by Data Controller as confidential, and will ensure that access to the Personal Data is limited to only those employees who require access to it for the purpose of Data Processor carrying out the permitted processing and complying with its obligations under this Agreement. Data Processor will ensure that all such employees have undergone adequate training.

2.4 **Information requests Data Subjects:** Data Processor agrees to assist Data Controller promptly with all subject information requests which may be received from the Data Subjects of the Personal Data within its service level target of 5 working days.

2.5 **Non-disclosure:** Data Processor will not disclose the Personal Data to a third party in any circumstances other than at the specific written request of Data Controller, unless the disclosure is required by law.

2.6 **Transfer of data outside EU:** Data Processor will only transfer the Personal Data outside of The European Union, if the country where the Personal Data is being transferred to provides an adequate level of protection of privacy that at least meets the minimal standards of European privacy protection, this includes implementation of the EU-US Privacy Shield. On request of Data Controller, Data Processor shall report to which countries the Personal Data will be transferred.

2.7 **Subcontracting:** Data Processor may sub-contract the processing of Personal Data to the following Sub-Processors: Active Campaign, Aircall, Amazon (AWS), Asana, AskNicely, Atlassian, Calendly, Dropbox, Freshdesk, Google, MailChimp, One, PandaDoc, PipeDrive, Postmark, Slack, Stripe, SurveyMonkey, Sync, Twinfield, Typeform, WHMCS, Woodpecker and Zapier. Data Processor may also engage other Sub-Processors, as long as Data Controller is informed about any intended changes and given the opportunity to object. These Sub-Processors must be appointed on the same terms as are set out in this Data Processing Agreement. On request of Data Controller, Data Processor will provide Data Controller insight into the data processing agreements that Data Processor has concluded with those parties. Data Processor will ensure that any Sub-Processor it uses to process the Personal Data, complies with the terms of this Agreement.

2.8 **Security measures:** Data Processor will employ appropriate operational and technological processes and procedures to keep the Personal Data safe from unauthorised use or access, loss, destruction, theft or disclosure. Data Processor will at least take the following security measures with regard to Personal Data:

- The network connection is secured with Secure Socket Layer (SSL) technology.
- All personal data is encrypted.
- Access to databases and servers require Two Step Verification and is limited to employees who have access to the Personal Data on a need to know basis.

- 2.9 **Removable drives and devices:** Data Processor will not keep the Personal Data on any laptop or other removable drive or device unless that device is protected by being fully encrypted, and the use of the device or laptop is necessary for the provision of the services under this Agreement or the MSA.
- 2.10 **Security incidents:** Data Processor will notify Data Controller of any information security incident that may impact the processing of the Personal Data covered by this Agreement, immediately after discovering or becoming aware of any such incident. Following the report of the incident, Data Processor will cooperate with Data Controller's Compliance and Information Security staff whilst they carry out a risk assessment, root cause analysis and identify any corrective action required. Data Processor will cooperate with Data Controller in implementing any required corrective action, agreed between the Parties.
- 2.11 **Removal of data after termination or cancellation:** On termination or cancellation of this Agreement, Data Processor will ensure that the Personal Data are securely removed from its systems and any printed copies are securely destroyed. In complying with this clause, electronic copies of the Personal Data shall be securely destroyed by either physical destruction of the storage media or secure deletion using appropriate electronic shredding software. Any hard copy will be destroyed by cross-cut shredding and secure re-cycling of the resulting paper waste. Also, after termination or cancellation of this Agreement, Data Processor may continue to use and possess generic aggregated data (the Personal Data that is irreversibly anonymized) for industry analysis and the improvement of the functionalities of its website.
- 2.12 **Audit:** Data Controller reserves the right to carry out compliance- and information security audits with regard to the practice of Data Processor, in order to satisfy itself that Data Processor is adhering to the terms of this Agreement, but only upon giving reasonable notice and within normal business hours.
- 2.13 **Indemnities and Liability:** Data Processor shall indemnify Data Controller against all damages which Data Controller may suffer arising out of any breach of this Agreement by Data Processor, for which Data Processor is liable. Data Processor shall be liable for such damages only when they are caused by (i) not complying with directly applicable obligations for Data Processors under the Relevant Privacy Legislation; or (ii) departing from the instructions of the Data Controller. Data Processor is not responsible or liable for any damages and loss which result from following instructions of Data Controller that do not comply with the Relevant Privacy Legislation.

3 **Governing Law**

- 3.1 This Agreement is exclusively governed by the laws of The Netherlands. Any disputes or claims arising out of or related to this Agreement shall exclusively be submitted to the competent court in Amsterdam.

4 **Term, amendment, termination or cancellation**

- 4.1 This Agreement shall become effective upon acceptance by Client and continues in full force and effect for the same period as the MSA, unless terminated for breach by either Party.
- 4.2 This Agreement embodies the entire understanding of the Parties with respect to the subject matter thereof. This Agreement supersedes previous agreements or understandings relating to this subject matter between the Parties, both in writing and oral, including correspondence. This Agreement may be modified or amended only by written agreement signed by both Parties.
- 4.3 Both Parties are entitled to cancel or terminate this Agreement with immediate effect in case the other Party does not adhere to the commitments made in this Agreement.
- 4.4 Any of the Parties may also terminate this Agreement with immediate effect in case of force majeure, including such a change in applicable laws and regulations that further continuation of the Agreement may reasonably not be required.



- 4.5 The termination or cancellation of this Agreement with immediate effect in accordance with the above provisions is done in writing, stating the reason for termination.
- 4.6 If any provision of this Agreement shall be deemed unlawful, void or otherwise unenforceable, then such provision shall be deemed severable from this Agreement and shall not affect the validity and enforceability of any remaining provisions. Any such unenforceable provision shall be replaced or be deemed to be replaced by a provision that is considered to be valid and enforceable and which interpretation shall be as close as possible to the intent of the invalid provision.