DATA PROCESSOR AGREEMENT

The undersigned:

1. Afdeling Online, with its registered office in Helmond and its principal place of business at 2e Haagstraat 40, 5707 VK Helmond, hereinafter referred to as the Processor, herewith duly represented by Jaap Schepers, Director,

2. The client, hereinafter referred to as the Controller,

   Also referred to jointly hereinafter as the Parties,

Whereas:

- The Controller wishes to utilise the services provided by the Processor in relation to the online marketing activities and/or web application or applications managed by the Processor.
- The Parties have signed a separate agreement relating to the service to be provided by the Processor to this end.
- The Processor will process personal data (hereinafter: Personal Data) for the Controller within the meaning of the Personal Data Protection Act (Wet bescherming persoonsgegevens (hereinafter: wbp)) within the framework of the agreement and the General Data Protection Regulation (hereinafter: GDPR).
- The Parties wish to set out a number of conditions in the present additional agreement (hereinafter: the Data Processor Agreement) that apply to the relationship between them in connection with the aforementioned activities, as instructed by and for the Controller - which they also wish to do in implementation of the provisions of Section 14(2) of the Wbp and Article 28(3) of the GDPR;
- The definitions of the terms 'Processor', 'Controller', 'Personal Data', 'process' and 'processing' used in the present agreement correspond with the definitions applicable in Section 1 of the Wbp and Article 4 of the GDPR;
- The Parties are aware that the Wbp will apply to this Data Processor Agreement until 25 May 2018, after which it will be governed by the GDPR from 25 May 2018 onwards. Both parties intend to comply with applicable legislation by entering into the present Data Processor Agreement.

Declare that they have agreed as follows:

Article 1 Subject of the Data Processor Agreement

1. The Controller will be responsible for processing Personal Data within the context of the performance of the agreement. The Processor will not have any independent control over the Personal Data.
2. The Processor will only process Personal Data when instructed to do so by the Controller within the context of the performance of the agreement, in accordance with the purposes and resources specified by the Controller, the retention periods described in Schedule 1 and also in accordance with any other written instructions issued by the Controller, except where a provision of Union or Member State law applicable to the Processor obliges the Processor to process Personal Data, in which situation the Processor will notify the Controller of the

statutory provision in question prior to processing, except where the legislation in question prohibits a notification of this nature on important grounds of public interest.
3. The Controller will guarantee that the instructions it issues to the Processor will result in processing by the Processor in accordance with applicable regulations and without infringing any rights of third parties.

Article 2 Technical and organisational provisions (security)

1. The Controller will only make Personal Data available to the Processor for processing if the Controller has satisfied itself that the security measures required have been put in place and, also bearing in mind the provisions of Article 32 of the GDPR, guarantee an appropriate level of protection, given the state of the art and the cost of implementation, this in view of the risks associated with processing and the nature of the data to be protected. An overview of security measures has been included in Schedule 2.
2. The Controller will be entitled to inspect the measures put in place and also compliance with the obligations to which the Processor is subject. The Controller will bear all costs, payments and expenses arising in connection with an inspection.
3. If the Processor has become aware of a security breach as described in Section 34a of the Wbp and/or Article 4(12) of the GDPR (hereinafter: Data Leak), the Processor will notify the Controller in writing as soon as possible. Where possible, it will do so within 24 (twenty-four) hours of the time at which the Data Leak came to the attention of the Processor.
4. The Processor will provide the Controller with information about the following at the very least: (i) the nature of the breach, where possible stating the categories of the data subjects in question and the approximate number of data subjects; (ii) the personal data possibly affected and the approximate amount of personal data affected; (iv) the measures that the Processor has taken and will take to address the breach, including, where appropriate, measures to limit any negative consequences of the breach.
5. The Processor recognises that, in certain circumstances, the Controller is required by law to notify data subjects or authorities of a security breach of whatever nature that relates or could relate (in part) to the Personal Data that the Processor processes. A notification of this nature by the Controller will never be deemed to be a failure in the performance of this agreement, or the underlying agreement, or otherwise a wrongful or unlawful act.
6. If a Data Leak happens despite the measures taken by the Processor, as agreed with the Controller, the Controller will not be able to hold the Processor liable for any losses sustained by the Controller as a result.

Article 3 Engaging third parties

1. The Processor will not outsource the obligations ensuing for it from the agreement to third parties, except where the Controller has given its prior written permission for the Processor to do so.
2. The Processor will require any subprocessors to comply with the provisions of the Data Processor Agreement. The Processor will utilise the services of the subprocessors identified in Schedule 1. The Processor will continue to be responsible for the acts and/or omissions of the subprocessors at all times.

Article 4 Transfer to third countries/the provision of Personal Data to third parties/requests from data subjects

1. The Processor will not be permitted to transfer Personal Data and/or to store it or have it stored in countries outside the European Union, except where the Processor has the explicit written consent of the Controller to do so and where permitted by applicable (European) privacy legislation. This could be because the country in question offers an appropriate level of

protection or an unamended model contract approved by the European Commission (hereinafter: EC Model Contract) is used to this end, with due observance of the other provisions of the Data Processor Agreement.

2. If Personal Data is transferred to the Processor or a third party in a country without an appropriate level of protection with the consent of the Controller, an unamended EC Model Contract will apply to this transfer. It will be signed by the Processor and enclosed with the Data Processor Agreement. The Processor will guarantee that all subprocessors that are engaged with the consent of the Controller will sign the EC Model Contract too.
3. The Processor will not provide Personal Data to an arbitrary third party, or make the said Personal Data available to an arbitrary third party, except where it does so by virtue of an explicit written instruction from the Controller or a demand from a judicial or administrative authority, provided the Processor notifies the Controller of the receipt of a demand of this nature within 24 hours, as such putting the Controller in a position to utilise the legal resource open to it against the aforementioned demand.
4. If the Processor is of the opinion that a legal obligation requires it to make Personal Data available to a competent authority, it will not proceed to do so before consulting and obtaining the written approval of the Controller. The Processor will notify the Controller as soon as possible in writing of the aforementioned legal obligation, also providing all relevant information that the Controller will reasonably need to take the measures required to determine whether Personal Data can be provided and, if yes, subject to which conditions.
5. The Processor will be required to notify the Controller in writing of all requests received directly from data subjects with regard to the rights that data subjects have under applicable privacy legislation, including but not limited to requests to inspect, rectify, delete or limit the processing or transfer of Personal Data. The Processor will only comply with a request of this nature if the Controller has explicitly instructed the Processor to do so in writing. The Controller is and will continue to be responsible for the consequences of its decisions in this respect. The Controller will indemnify the Processor against any claims from data subjects in this respect.

Article 5 Rendering assistance

1. Taking into consideration the nature of the processing, the Processor will, wherever possible, assist the Controller by taking appropriate technical and organisational measures that the Controller needs to be able to respond to the requests of data subjects whose Personal Data are being processed as referred to in Sections 35 and 36 of the Wbp and Chapter III of the GDPR and also requests from the regulatory authority with competence in relation to the Controller.
2. Taking into consideration the nature of the processing and the information available to it, the Processor will help the Controller to fulfil the obligations ensuing from Articles 32 up to and including 36 of the GDPR, in relation to which the Processor is entitled to charge the Controller for all reasonable costs, where applicable.

Article 6 Confidentiality

1. The Processor and all of its employees who have access to Personal Data will maintain the confidentiality of the Personal Data of which they take note, except where a statutory provision requires them to disclose Personal Data.
2. The Processor will ensure that all of its employees who are involved in performance of the agreement sign a non-disclosure agreement. The Processor will take all measures that are necessary to guarantee that this duty of confidentiality is honoured.

Article 7 Provision and deletion

As required by the Controller, the Processor will delete or return all Personal Data to the Controller within six months of the date on which the agreement is terminated. The Processor will also delete all existing copies within the same time frame, except where the retention of Personal Data is required by current regulations.

Article 8 Liability

1. If the Processor is liable to the Controller for losses for whatever reason, the Processor will only be liable for direct losses that the Controller sustains as the result of an attributable failure and/or wrongful and/or unlawful act, without prejudice to the provisions of Article 2(4). The total liability applicable under the agreement, including the Data Processor Agreement, or infringement by the Processor and/or the subprocessor or subprocessors of the relevant (European) privacy legislation, will never exceeded an amount of € 5,000.
2. The Processor will never be liable for consequential loss, also including loss of a purely financial nature, lost profits and intangible loss. The Processor will particularly not be liable for losses in connection with and/or as the result of:
    a. the ending of or changes to the service provided;
    b. communication shortcomings in connection with hardware, software, network or other computer problems;
    c. the use of data or data files stipulated by the Controller;
    d. the loss, corruption or destruction of data or data files; and/or,
    e. the inaccessibility of the service provided by Processor.
3. If performance is not permanently impossible, the Processor will only be liable for a demonstrable attributable failure to perform the Data Processor Agreement if the Controller issues the Processor with a notice of default immediately, properly and in writing, giving the Processor a reasonable period of time in which to rectify the failure, and the Processor continues to attributably fail to fulfil its obligations even after the expiry of the said reasonable period. The notice of default must include a description of the failure that is as full and detailed as possible, so that the processor is in a position to respond adequately.
4. A right to compensation will only ever arise if the Controller reports the loss to the Processor in writing as soon as possible after the occurrence thereof. Any claim for compensation against the Processor will expire six (6) months after the date on which the claim arose.

Article 9 Inspection and regulation/transferring rights and obligations

The Controller will be entitled to inspect measures and compliance with the obligations to which the Processor is subject, which the Controller will do at its own expense, provided the Controller notifies the Processor of an inspection five (5) working days in advance and on the condition that the Controller observes the reasonable instructions of the Processor during the inspection and the inspection does not unreasonably disrupt the business operations of the Processor.

The Controller is the controller described in Article Section 4(7) of the GDPR as regards the processing of Personal Data under this agreement. The Controller agrees to and guarantees that processing of the Personal Data in conformity with this agreement is in accordance with the applicable privacy legislation.

The Processor may not transfer this agreement or the rights and obligations ensuing from it to third parties without the prior written consent of the Controller.

Article 10 Other provisions

1. In the event of inconsistencies between (one or more provisions of) the Data Processor Agreement with (one or more provisions from) other agreements between the Controller and the Processor, the Data Processor Agreement will prevail.
2. This agreement will have the same term as that applicable for the underlying agreement and may not be terminated early. Articles that are such that the intention is for them to remain in force even when the Data Processor Agreement ends, one such article being the article relating to fulfilment of the Data Processor Agreement, which articles will include - but not be limited to - Article 6 (Confidentiality), Article 7 (Provision and deletion) and Article 10(5) and (6), will remain in full force following the termination of the Data Processor Agreement.
3. It will only be possible to amend the Data Processor Agreement if both Parties agree to the amendment in question in writing.
4. Should any provision of the Data Processor Agreement be nullified or declared void, or if it transpires that a change in circumstances makes it necessary to amend (a provision of) the Data Processor Agreement in order to maintain compliance with applicable privacy-related legislation and regulations, the other provisions will remain in full force. The Parties will then establish a new provision to replace the nullified/voided provision or amend the Data Processor Agreement such that it is in line with applicable privacy-related legislation and regulations again, taking into consideration the purport of the nullified/voided provision.
5. Dutch law will apply to the Data Processor Agreement.
6. Disputes between the Controller and the Processor will exclusively be submitted to the competent court in the court district of Rotterdam.

Schedule 1

Data will be processed by the Processor with the following **purposes** in mind:

1. The performance of online marketing activities designed to promote and analyse the Controller. The development and maintenance of a web application or applications being managed by the Processor.
2. The performance of activities that are necessary to realize the development and testing of a web application or applications.
3. Displaying the appropriate content to the user on the basis of rights and roles.

Processing **resources** will include the following:

1. (Web) servers (DTAP roadmap).
2. Hosting software and hardware.
3. Hardware that employees of the Processor use to carry out online marketing and develop and manage an application or applications.
4. Network supplier and hosting provider.
5. Software implementation for the purpose of performance monitoring and (user) statistics.

Type of personal data to be processed:
All traceable (non-anonymised) personal data that is processed in the web application or applications will fall under this Data Processor Agreement

Retention periods
Data will be retained throughout the term of the agreement entered into, except where agreed otherwise in the principal agreement.

Use of the data
The Processor will only process data at the request of the Controller, in relation to the analysis, management, promotion and further development of the web application.

Provision to third parties
The Processor will not provide any data to third parties, except where ordered to do so by a competent government body.

Subprocessors
- Google - Analytics, Ads, Doubleclick, Analyze, Tag Manager, Data Studio
- Facebook - Facebook & Instagram Community management & advertising
- Linkedin - Community management & Advertising
- Twitter - Community management & Advertising
- Swydo - Reports
- SE Ranking - SEO reports
- Hootsuite - Social monitoring and reports
- VDX Internet Services - Domain names, e-mail boxes and SSL
- Redkiwi - Web development
- Mailchimp - Email marketing
- Hotjar Ltd. - Analytics

The Processor uses the services of freelancers and plugin developers for web development purposes on an incidental basis. However, they have no access, or just limited access, to production environments containing personal data.

Schedule 2

Overview of the security measures requested by the Controller

An overview follows below of the security measures that the Processor puts in place. These measures are subject to change, but changes must not result in a lower level of general security.

Security
- The Processor operates a system of user rights, which limits access to data to employees and job holders that need this access. Processes like the off-boarding process have been defined too, to ensure that user rights are withdrawn when an employee leaves the employment of the Processor.
- The Processor will secure the accounts, software and application or applications with both technical and organisational aspects in mind and will, at the very least, achieve a level of security that is appropriate and reasonable given the state of the art, the sensitivity of the (personal) data and the cost of the security in question.
- The Processor will make the use of encrypted connections (SSL) compulsory when sending data and files from and to the web application.
- The Processor will update the server software and the application. The Processor will also monitor the server and application.
- The Processor will make it compulsory to upgrade and update the software used. If the Controller decides not to update software, this agreement will cease to be valid.

Hosting
Afdeling Online uses hosting suppliers, with which the following agreements have been made.
- Back up: Data and source files are backed up on a monthly basis. The retention period for backups is three months. We use Google Cloud Storage for this purpose in Europe.

- Availability: The datacenter features emergency power supplies and has a number of internet connections.
- The hosting provider will ensure that network security and physical security are in place for the servers (including access control).