DATA PROCESSING AGREEMENT

(Hereafter referred to as “DPA” or “Agreement”)

completed between the

- Responsible (the “Controller”) -

_____ organised and existing under the laws of _____, with Registered Business No. _____, VAT No.: _____, with its registered office at _____, represented by _____, director

and

- processor (the “Processor”) -

Niteo GmbH organised and existing under the laws of Principality of Liechtenstein, with Registered Business No. FL-0002.587.864-6, VAT No.: 60671, with its registered office at Landstrasse 15, 9496 Balzers, represented by Marbe Ann Ralozo, director

shall be effective on the later date set down below (“Effective Date”).

The Controller and the Processor are hereinafter jointly referred to as the “Parties” or individually as the “Party”.

This DPA is part of the Terms of Service, Privacy Policy and other relevant policies available on the website: https://niteo.co/legal/terms.

Preamble

This appendix specifies the contractual obligations of the Parties to data protection arising from the order processing described in detail in the Contract. It applies to all activities that are related to the Contract and in which employees of the Processor process personal data (hereinafter referred to as "Data") of the Controller.

“The Contract” shall mean the services agreement entered into between the Controller and Processor, dated _____, (“Effective date”).

Definitions

The "Controller", the "Processor", "Data Subject", "Processing", "Personal Data", "Personal Data Breach" shall have the meanings ascribed to them in Data Protection Laws.

"Client Personal Data" means any Personal Data subject to the Data Protection Laws that the Controller provides, transfers or makes accessible to the Processor in connection with the Services.

"Data Protection Laws" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and any similar or related implementing legislation by European Union or European Economic Area member states, the United Kingdom or Switzerland. The Parties also acknowledge that non-European Data Protection Laws may also apply to the processing of Customer Personal Data.

§ 1 Subject, duration, purpose and specification of processing

(1) The purpose and duration of the Contract as well as the nature and purpose of the processing arise from the Contract. In particular, the following data is part of the data processing:

Type of data: customer email, customer, location, customer payment and order details

Type and purpose of the data processing: web hosting, web analytics, payment processing

Categories of affected persons: customers, contact persons

(2) The Duration of processing depends on the duration of the Contract.

§ 2 Scope and responsibility

(1) The Processor processes Personal Data on behalf of the Controller and performs services on behalf of the Controller in accordance with the Contract. This includes activities that are specified in the Contract, this DPA and in the specifications. Within the scope of this contract, the Controller is solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the legality of the data transfer to the Processor and for the lawfulness of the data processing,

(2) When providing services, the Processor collects, uses or otherwise process Personal Data within the meaning of the Data Protection Laws and Regulations for which the Controller is responsible as provided under the said Data Protection Laws.

(3) This DPA regulates the data protection obligations of the Parties when processing Personal Data of the Controller, under the Contract and shall ensure that such processing will only take place on behalf of and under the instructions of the Controller and in accordance with the Data Protection Laws, including but not limited to Article 28 of the GDPR.

(4) The instructions are initially determined by the Contract and can then be amended, supplemented, or replaced by the Controller in written form or in an electronic format (text form) to the body designated by the Processor by individual instructions. Instructions that are not provided for in the contract are treated as an application for a change in performance. Verbal instructions must be confirmed immediately in writing or in text form.

§ 3 Obligations of the Processor

(1) The Processor may process data of affected persons only within the framework of the order and the written instructions of the Controller. The Processor informs the Controller immediately if he believes that a directive violates applicable laws. The Processor may suspend the implementation of the instructions until they have been confirmed or modified by the Controller.

(2) If the Processor receives an official order to publish data of the Controller, he shall - insofar as legally permissible - inform the Controller immediately and refer the authority to the latter. Similarly, processing the data for the processor's own purposes requires a written order.

(3) The Processor will, in his area of responsibility, design the in-house organization in such a way that it meets the special requirements of data protection. Technical and organizational measures shall be taken to adequately protect the data of the Controller, which meet the requirements of the General Data Protection Regulation (Art. 32 of the GDPR). The Processor shall take technical and organizational measures to ensure the confidentiality, integrity, availability and resilience of the systems and services related to the processing on a permanent basis.

(4) The Controller shall be made aware of these technical and organizational measures in writing and shall be held responsible for ensuring that they provide an adequate level of protection for the risks of the data to be processed.

(5) The Processor shall support the Controller as far as possible in fulfilling the inquiries and claims of data subjects in accordance with Chapter III of the GDPR (right to information, information, correction and deletion, data portability, objection and automated decision - making in individual cases) as well as to the compliance with the obligations set out in Articles 32 to 36 of the GDPR (data security measures, notification of data breaches to the supervisory authority, notification of the data subject of a data breach, data protection impact assessment, prior consultation).

(6) The Processor warrants that the employees involved in the processing of the data of the Processor and other persons working for the Processor shall be prohibited from processing the data out of scope of instructions passed on to them. Furthermore, the Processor guarantees that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate legal secrecy obligation. The obligation of confidentiality / secrecy persists even after the order has been completed.

(7) The Processor shall inform the Controller without undue delay if he becomes aware of violations of the protection of personal data of the Controller. The Processor shall take the necessary measures to secure the data and to reduce the possible adverse consequences of the persons concerned and shall immediately discuss this with the Controller.

(8) The Processor shall inform the Controller of the contact person for data protection issues arising in the context of the contract.

(9) The Processor shall also ensure that obligations under Article 32 (1) (d) of the GDPR are fulfilled and that a periodic review of the effectiveness of the technical and organizational measures to ensure the safety of the processing is concluded. With regards to the processing of the data provided by the customer, the customer is granted the right to inspect and control at any time, even if third parties commissioned by him, to the data processing facilities. The Processor undertakes to provide the Controller with the information necessary to control compliance with the obligations set out in this Agreement.

(10) The Processor rectifies or deletes the contractual data if the Controller so instructs and this is included in the scope of the directive. If a data protection confirming deletion or a

corresponding limitation of the data processing is not possible, the processor takes over the data protection compliant destruction of data media and other materials on the basis of an individual commissioning by the Controller or returns these data carriers to the Controller, if not already agreed in the contract.

(11) The processing of data in private homes is permitted only with the consent of the Controller in individual cases. As far as the data are processed in a private apartment, the access to the apartment by the Controller must be coordinated in advance with the processor. The Processor assures that the other residents of this private dwelling agree with this regulation.

(12) Data, data carriers as well as all other materials shall either be issued or deleted after the end of the order at the request of the Controller. If the Processor processes the data in a special technical format, it is obliged to provide the data after termination of this agreement either in this format or at the request of the Controller in the format in which the data from the Controller has been received, common Format issue. If additional costs arise as a result of deviating specifications in the case of the publication or deletion of the data, the costs shall be covered by the Controller.

(13) In the case of a claim of the customer by an affected person with regards to any claims under Art. 82 GDPR (compensation for damages), the Processor undertakes to assist the Controller in defending the claim to the extent possible.

§ 4 Obligations of the Controller

(1) The Controller must inform the Processor immediately and in full should it be discovered that the order results errors or irregularities regarding data protection regulations.

(2) The Controller is responsible for fulfilling the obligations pertaining solely to the Controller in particular order to ensure compliance with the Data Protection Laws.

(3) The Controller shall provide all required and relevant instructions to the Processor in a timely, sufficiently, clear and detailed matter in either written or electronic form.

(4) The Controller shall confirm in writing any verbal instructions given to the Processor as soon is reasonably possible after such instructions are originally given.

(5) In case of a claim of the Processor by an affected person in regards to any claims under Art. 82 GDPR, § 3 (11) shall apply mutatis mutandis.

(6) The Controller shall provide the Processor contact information of a person responsible for data protection issues arising in the context of the contract.

§ 5 Requests of affected persons

(1) Should an affected person file claims for correction deletion or information with the Processor, the Processor shall refer the person concerned to the Controller, if an assignment to the Controller according to the data subject is possible. The Processor forwards such claims to the Controller immediately. The Processor supports the Controller as far as possible within the scope of his possibilities. The Processor shall not be held liable if the request of the data subject is not answered by the Controller, not correctly or not in time.

§ 6 Place of execution of data processing

Data processing activities are carried out, at least in part, outside the EU / EEA, in United States. The appropriate level of data protection results from Privacy Shield Framework (https://www.privacyshield.gov/).

§ 7 Detection options

(1) The Processor shall present the Controller information and materials proving the compliance with the obligations laid down in this Agreement by suitable means. The Processor is carrying out self-audits and has a Corporate Code of Conduct.

(2) If, in individual cases, inspections by the Controller or an inspector commissioned by the latter are required, they shall be carried out during normal business hours without disruption to the operation after registration, taking into account a reasonable lead time. The Processor may make these dependent on prior notification with reasonable lead time and on the signing of a confidentiality agreement regarding the data of other customers and the technical and organizational measures that have been set up. If the examiner commissioned by the Controller is in a competitive relationship with the Processor, the processor has a right to appeal.

(3) If a data protection supervisory authority or another sovereign supervisory authority of the Controller carries out an inspection, paragraph 2 shall apply accordingly. A signing of a confidentiality obligation is not required if this supervisory authority is subject to a professional or legal secrecy, in which a violation under the Criminal Code is punishable.

§ 8 Subprocessors

(1) The Processor is allowed to engage third party subcontractors that process Personal Data ("Subprocessors") for the purposes of providing the Services.

(2) A Subprocessor agreement subject to approval exists if the Processor commissions further Processors providing all or parts of the performance agreed in the Contract. The Processor will make agreements with these third parties to the extent necessary to ensure adequate privacy and information security measures. The Processor shall impose obligations on Subprocessors that are the same as or substantially equivalent to those set out in this Agreement by way of written contract.

The contractually agreed services or partial services described below are carried out with the involvement of the following Subprocessors:

- Facebook, 1 Hacker Way in Menlo Park, CA 94025, USA; web analytics and customer location; data processed: customer location; https://www.facebook.com/legal/terms/dataprocessing
- Google LLC, Google Ireland Limited, Google Asia Pacific Pte. Ltd.; web hosting, web analytics; data processed: live data and backups; https://cloud.google.com/terms/data-processing-terms
- Heroku, Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, USA; web application hosting; data processed: customer email and location; https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf

- Mixpanel, 405 Howard St 2nd Floor, San Francisco, USA; website analytics; data processed: customer email and location; https://mixpanel.com/legal/dpa/
- Paddle.com Market Ltd, 15 Bermondsey Square, 1st Floor London SE1 3UN, United Kingdom; payment provider and merchant of record; data processed: customer email, location and payment details; https://paddle.com/gdpr/
- SendGrid Inc.,1801 California St #500, Denver, USA; email service provider; data processed: transactional emails; https://s3.eu-west-2.amazonaws.com/primalbase/privacy/SEND+GRID+data+contract.pdf

Prior to the involvement of further or the replacement of listed Subprocessors, the Processor shall get the consent from the Controller, which may not be denied without presenting important data protection reason.

§ 9 Liability and damages

(1) The Controller shall be held liable for damages to the concerned data subjects caused by processing of personal data which is not compliant with the Data protection Laws and which are not caused by the acts or omissions of the Processor.

§ 10 Duration

(1) The rights, benefits and obligations of this DPA shall commence on the date of signature by both Parties of this DPA and shall terminate with the termination of the services under the Contract.

§ 11 Information obligations, written form clause, choice of law

(1) Should the data of the Controller be endangered by seizure, by a bankruptcy or settlement procedure or by other events or measures of third parties, the Processor shall inform the Controller of such situation without delay. The Processor will immediately inform all those responsible, that the sovereignty and the ownership of the data are exclusively the responsibility of the Controller in the sense of the General Data Protection Regulation.

(2) Amendments and additions to this Agreement and all of its components require a written agreement, which may also be in an electronic format (textual form), and an explicit indication that it is an amendment or modification supplementing these conditions. This also applies to the waiver of this form requirement.

(3) In the case of any contradictions, regulations on data protection of this Agreement shall take precedence over the provisions of the Contract. Should individual parts of this Agreement be ineffective or void, this does not affect the effectiveness of other parts the Agreement.

(4) The applicable law is the law of Principality of Liechtenstein.

Information in accordance with § 3 (8):

The processor is the data protection officer

Marbe Ann Ralozo, gdpr@niteo.co. A change is to be communicated to the controller immediately.

Information according to § 4 (6):

The controller is the person responsible for data protection

_____, _____. A change is to be communicated to the processor immediately.

Processor Niteo GmbH, represented by (name) Marbe Ann Ralozo

Date 2020/01/01

Controller _____, represented by (name) _____,

Date _____,

ANNEX 1

Technical and organizational measures

The Processor shall implement and maintain appropriate technical and organisational security measures for processing of Personal Data, including the measures set out in this Annex, to ensure a level of security appropriate to the risk, including but not limited as appropriate:

- The pseudonymisation and encryption of personal data,
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services,
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident,
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access and all other unlawful forms of processing. Additional measures and relevant information concerning such measures, including the specific security measures and practices for the services agreed upon may be specified in this Agreement.

The Processor and Subprocessors employ strict procedures for reuse, redeployment, data destruction and decommission of disks and hardware and ensure that all the unnecessary data and data, for which any lawful reason to be processed no longer exists is deleted.

The Processor ensures that login credentials are rotated regularly, in 90 day intervals.

The Processor ensures that all contractor and employee account accesses are reviewed regularly, every 90 days.

The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and the Contract and will allow for quarterly audits.

The Processor may update or modify these Technical and organisational measures as needed, provided that such updates and modifications do not result in the degradation of the overall security of the services.

Employees and Confidentiality

The Processor shall be taking all the precautions and steps necessary to protect all Personal Data processed.

The Processor shall take reasonable steps to ensure that no person shall be allowed to process Personal Data, unless that person is:

- competent and qualified to perform the tasks assigned to them by the Processor;
- has been authorised by the Processor;
- has been instructed and educated by the Processor of all requirements relevant to the performance of the obligations of the Processor under these Clauses, particularly the limited purpose of the data processing.

Employees of the Processor are required to conduct themselves in a manner consistent with the guidelines and training provided by the Processor, regarding confidentiality, business ethics,

appropriate usage and professional standards. Employees shall enter into a confidentiality agreement with the Processor and shall acknowledge compliance with Privacy and Confidentiality policies of the Processor. All employees shall follow the rules set and described in detail in the Security Policy, available on the page: https://github.com/niteoweb/handbook/blob/master/2_Operations/security.md

Physical Security and System Access Control

The Processor stores all data in physically secure data centres. The Processor and Subprocessors employ measures to secure the access to data processing systems. The access system that controls access to the data centre is in place and permits only authorised personnel to have access to the secure areas.

The Processor maintains a security policy for their employees. The Processor has designed internal access processes and policies to prevent unauthorized persons from gaining access to the personnel data. Systems of the Processor are designed to only allow authorized persons to access data they are authorized to access and to ensure that Personal Data cannot be read, copied, altered or removed without authorization during processing, use and after recording.

Subprocessor security

Before onboarding Subprocessors, the Processor conducts an audit of the security and privacy practices of Subprocessors to ensure they provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. The Subprocessor shall enter into appropriate security, confidentiality and privacy contract terms.

Processor Niteo GmbH, represented by (name) Marbe Ann Ralozo

Date 2020/01/01

Controller _____, represented by (name) _____,

Date _____,