Nebu B.V.
Pakhuisplein 42 V
1531 MZ Wormer
The Netherlands
T: + 31 251 311413
E: nebu@nebu.com
W: www.nebu.com

Nebu Data Processing Agreement

(DPA)

Reference	:	Nebu - I-2019 - 0075
Version	:	1.1
Date	:	December 16, 2019
Owner	:	Otto van Linden
Validation:	:	Zoltan Szuhai
Status	:	Final
Qualification	:	Public

CONTENTS

1 Introduction 3

2 Definitions 4

3 Scope and Responsibility 5

4 Obligations of Processor 6

5 Obligations of Controller 8

6 Enquiries by Data Subjects to Controller 9

7 Audit Obligations 10

8 Subcontractors 11

9 Additional Terms 12

Exhibit A. List of Subcontractors 13

Version Control			
Version	**Status**	**Date**	**Change Log**
V1.0	Final	February 12, 2018	-
V1.1	Final	December 16, 2019	Textual corrections and minor content changes

1 Introduction

This Nebu Data Processing Agreement ("***DPA***") reflects the ***Parties'*** agreement with respect to the terms governing the processing of ***Personal Data*** under the Nebu General term & Conditions (the "***Agreement***"). This ***DPA*** is a supplement to the ***Agreement*** and is effective from January 1, 2018.

The main purposes of this addendum is to accommodate:

"***REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*** *of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, and repealing Directive 95/46/EC (General Data Protection Regulation)

for ***Customers*** located in the European Union or the European Economic Area to further provide adequate safeguards with respect to the data processed under the ***Agreement***. Having said that, Nebu will take an integral approach and will apply all processes for all its ***Customers*** irrespective of residency of the ***Customer***.

In all cases ***Nebu*** ("***Processor***"), or a third party acting on behalf of ***Processor***, acts as the processor of ***Personal Data*** and ***Customer*** ("***Controller***") remains controller of ***Personal Data***. It is recognized that you, our ***Customer***, is might be processing information on behalf of your customers ***("End-Customers")*** in which case ***Nebu*** is a ***Sub-Processor, Customer*** is ***Processor*** and the ***End-Customer Controller*** Within such a situation, it is deemed that ***Customer*** is action to ***Nebu*** on behalf of the ***Controller*** and all obligations are unchanged, but transferred.

Terms not otherwise defined herein shall have the meaning as set forth in the ***Agreement***.

2 Definitions

(i) "***Customer Data***" means all information that ***Customer*** submits, collects, generates or processes via the ***Nebu Services***.

(ii) "***Personal Data***" means any individual element of information concerning the personal or material circumstances of an identified or identifiable individual.

(iii) "***Processing***" means processing of ***Personal Data*** on behalf, encompassing the storage, amendment, transfer, blocking or erasure of personal data by the ***Processor*** acting on behalf of the ***Controller***.

(iv) "***Instruction***" means the written instruction, issued by ***Controller*** to ***Processor***, and directing the same to perform a specific action on ***Personal Data*** (including, but not limited to, depersonalising, blocking, deletion, making available). Instructions shall initially be specified in the ***Agreement*** and may, from time to time thereafter, be amended, amplified or replaced by ***Controller*** in separate written instructions (individual instructions).

(v) "***Sensitive Information***" means (a) credit or debit card numbers; personal financial account information; Social Security numbers or local equivalents; passport numbers; driver's license numbers or similar identifiers; passwords; racial or ethnic origin; physical or mental health condition or information; or other employment, financial or health information, including any information covered by regulations, laws or industry standards designed to protect similar information; and (b) any information defined under ***GDPR*** (Article 9) data protection laws as 'special categories of personal data.

(vi) "***Users***" means ***Customers'*** employees, representatives, consultants, contractors or agents who are authorized to use the ***Nebu Services*** for your benefit and have unique user identifications and passwords for the ***Nebu Services***.

3 Scope and Responsibility

3.1 The main purpose of the ***Nebu Services*** is to allow ***Customers*** to collect, manage & utilise (i.e. ***Processing***) data for market(ing) research purposes. Within the collection a core functionality is that information can be collected from individuals, typically requiring ***Personal Data*** (also referred to as "*Sample Data*") to initiate or to be collected as part of the ***Customer Data***. ***Parties*** acknowledge, that it is non-trivial to discern ***Personal Data*** within the ***Customer Data***, as such any ***Customer Data*** will be treated by ***Nebu*** as ***Personal Data***.

3.2 ***Processor*** shall process ***Customer Data***, which might include ***Personal Data***, on behalf of ***Controller***. ***Processing*** shall include such actions as may be specified in the ***Agreement*** and/or an ***Order***.

3.3 Within the scope of the ***Agreement****, and provided* ***Nebu*** *performs its obligations under this Agreement*, ***Controller*** shall be solely responsible and liable for complying with the statutory requirements relating to data protection, in particular regarding the transfer of ***Personal Data*** to the ***Processor*** and the ***Processing*** of ***Personal Data***.

3.4 Based on the responsibility of §3.3, ***Controller*** shall be entitled to demand and ***Processor*** shall subsequently execute, the rectification, deletion, blocking and making available ***of Personal Data*** during and after the term of the ***Agreement*** in accordance with the further specifications of such agreement on return and deletion of personal data.

3.5 The regulations of this ***DPA*** shall equally apply if testing or maintenance of automatic processes or of ***Processing*** equipment is performed on behalf of ***Controller***, and access to ***Personal Data*** in such context cannot be excluded.

4 Obligations of Processor

4.1 ***Processor*** shall collect, process and use ***Customer Data***, which might include ***Personal Data***, only within the scope of ***Controller's Instructions***.

4.2 If the ***Processor*** thinks that an instruction of the ***Controller*** infringes any data protection provisions, it shall point this out to the ***Controller*** without delay.

4.3 Within ***Processor's*** area of responsibility, ***Processor*** shall structure ***Processor's*** internal organisation to ensure compliance with the specific requirements of the protection of ***Personal Data***.

4.4 ***Processor*** shall, taking into account the nature of ***Processing*** and insofar as this is reasonable possible take the appropriate technical and organisational measures to adequately protect ***Controller's Customer data***, which might include ***Personal Data***, against misuse and loss in accordance with the requirements of the ***GDPR***, or otherwise applicable national data protection law. Such measures will ensure a level of security appropriate to the risk taking into account the state of the art and the costs of implementation, in view of the risk entailed by ***Personal Data Processing*** and the nature of the data to be protected. Such measures shall include, but not be limited to:

(i) the prevention of unauthorized persons from gaining access to ***Customer Data***, which might include ***Personal Data,*** processing systems (physical access control),

(ii) the prevention of ***Customer Data***, which might include ***Personal Data,*** Processing systems from being used without authorization and/or unauthorised or unlawful processing (logical access control),

(iii) ensuring that persons entitled to use a ***Customer Data***, which might include ***Personal Data***, system gain access only to such ***Customer Data***, which might include ***Personal Data***, as they are entitled to accessing in accordance with their access rights, and that, in the course of processing or use and after storage, ***Customer Data***, which might include ***Personal Data***, cannot be read, copied, modified or deleted without authorization (data access control),

(iv) ensuring that ***Customer Data***, which might include ***Personal Data,*** cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of ***Customer Data***, which might include ***Personal Data,*** by means of data transmission facilities can be established and verified (data transfer control),

(v) ensuring the establishment of an audit trail to document whether and by whom ***Customer Data***, which might include ***Personal Data***, have been entered into, modified in, or removed (entry control),

(vi) ensuring that ***Customer Data***, which might include ***Personal Data***, are ***Processed*** solely in accordance with the ***Instructions*** (control of instructions),

(vii) ensuring that ***Customer Data***, which might include ***Personal Data***, are protected against accidental destruction, damage or loss (availability control),

(viii) ensuring that ***Customer Data***, which might include ***Personal Data***, collected for different purposes can be processed separately (separation control).

Nebu Services can be offered as a hosted service, but also as part of an on-premise installation. In case of on-premise installations, the ***Customer*** has control over the physical access control (i) and also (partially) on the elements (ii) to (viii) referred to above. In these cases, ***Nebu*** can only serve as an advisor and ensure that on engagement the organizational measures are being adhered to.

4.5 Upon ***Controller's*** request, ***Processor*** shall provide a current ***Personal Data*** protection and security programme covering ***Processing*** hereunder.

4.6 ***Processor*** shall ensure that any personnel entrusted with ***Processing Controller's Customer Data***, which might include ***Personal Data***, have undertaken to comply with the principle of data secrecy, which includes ensuring that persons authorised to process ***Personal Data*** have committed themselves to confidentiality, in accordance with ***GDPR*** and have been duly instructed on the protective regulations of the ***GDPR***. The undertaking to secrecy and confidentiality shall continue after the termination of the above-entitled activities.

4.7 The ***Processor*** shall appoint a ***Data Protection Officer***, if this is legally required and, upon request of ***Controller***, ***Processor*** shall notify to ***Controller*** the contact details of the ***Data Protection Officer***.

4.8 ***Processor*** shall, without undue delay, inform ***Controller*** in case of a serious interruption of operations or violations by the ***Processor*** or persons employed by it, of any provision or obligation of this ***DPA*** to protect ***Customer Data***, which might include ***Personal Data*** or of terms specified in this ***DPA***.

4.9 In such an event, ***Processor*** shall implement the measures necessary to secure the ***Customer Data***, which might include ***Personal Data***, and to mitigate potential adverse effects on the data subjects and shall agree upon the same with ***Controller*** without undue delay.

4.10 ***Processor*** shall support ***Controller*** in fulfilling ***Controller's*** disclosure obligations under ***GDPR*** (or a corresponding provision of the otherwise applicable national data protection law).

4.11 ***Controller*** shall retain title as to any carrier media provided to ***Processor*** as well as any copies or reproductions thereof. ***Processor*** shall store such media safely and protect them against unauthorised access by third parties.

4.12 ***Processor*** shall, upon ***Controller's*** request, provide to *Controller* all information on ***Controller's Customer Data***, which might include ***Personal Data***, and information.

4.13 ***Processor*** shall be obliged to securely delete any test and scrap material based on an ***Instruction*** issued by ***Controller*** on a case-by-case basis. Where ***Controller*** so decides, ***Processor*** shall hand over such material to ***Controller*** or store it on ***Controller's*** behalf.

4.14 ***Processor*** shall be obliged to audit and verify the fulfilment of the above-entitled obligations and shall maintain an adequate documentation of such verification.

5 Obligations of Controller

5.1 ***Controller*** and ***Processor*** shall be separately responsible for conforming with such statutory data protection regulations as are applicable to them.

5.2 ***Controller*** shall inform ***Processor*** without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the ***Processing*** of ***Customer Data***, which might include ***Personal Data***, detected during a verification of the results of such ***Processing***.

5.3 ***Controller*** shall be obliged to maintain the publicly available register or a corresponding provision) of the applicable national data protection law, if any.

5.4 ***Controller*** shall be responsible for fulfilling the duties to inform, both the ***Supervisory Authority*** and the ***Data Subject***, as per the ***GDPR*** or a corresponding provision of the otherwise applicable national data protection law.

5.5 ***Controller*** shall, upon termination or expiration of the ***Agreement*** and by way of issuing an ***Instruction***, stipulate, within a period of time set by ***Processor***, the reasonable measures to return data carrier media or to delete stored data.

5.6 Any additional cost arising in connection with the return or deletion of ***Customer Data***, which might include ***Personal Data***, after the termination or expiration of the ***Agreement*** shall be borne by ***Controller***.

6 Enquiries by Data Subjects to Controller

6.1 Where ***Controller***, based upon applicable data protection law, is obliged to provide information to an individual about the collection, processing or use of its ***Personal Data***, ***Processor*** shall assist ***Controller*** in making this information available, provided that:

(i) ***Controller*** has instructed ***Processor*** in writing to do so, and

(ii) ***Controller*** reimburses ***Processor*** for the costs arising from this assistance.

6.2 Where a ***Data Subject*** requests the ***Processor*** to correct or delete ***Personal Data***, ***Processor*** shall refer such data subject to the ***Controller***.

7 Audit Obligations

7.1 ***Controller*** shall have the right, prior to the commencement of ***Processing***, and/or at regular intervals thereafter, to audit the technical and organisational measures taken by ***Processor***, and if done so shall document the resulting findings.

7.2 For such purpose, ***Controller*** may, e.g.,

i. obtain information from the ***Processor***,

ii. request ***Processor*** to submit to ***Controller*** an existing attestation or certificate by an independent professional expert, or

iii. upon reasonable and timely advance agreement, during regular business hours and without interrupting ***Processor's*** business operations, conduct an on-site inspection of ***Processor's*** business operations or have the same conducted by a qualified third party which shall not be a competitor of ***Processor***.

7.3 ***Processor*** shall, upon ***Controller's*** written request and within a reasonable period of time, provide ***Controller*** with all information necessary for such audit.

8 Subcontractors

8.1 ***Processor*** shall be entitled to subcontract ***Processor's*** obligations defined in the ***Agreement*** to third parties only with ***Controller's*** written consent.

8.2 ***Controller*** consents to ***Processor's*** subcontracting to ***Processor's*** affiliated companies and third parties, as listed in Exhibit 2, of ***Processor's*** contractual obligations hereunder.

8.3 If the ***Processor*** intends to instruct subcontractors other than the companies listed in Exhibit 2, the ***Processor*** must notify the ***Controller*** thereof in writing (email to the email address(es) on record in ***Processor's*** account information for ***Controller*** is sufficient) and must give the ***Controller*** the possibility to object against the instruction of the subcontractor within 30 days after being notified.

8.4 The objection must be based on reasonable grounds (e.g. if the ***Controller*** proves that significant risks for the protection of its ***Personal Data*** exist at the subcontractor). If the ***Processor*** and ***Controller*** are unable to resolve such objection, either party may terminate the ***Agreement*** by providing written notice to the other party. ***Controller*** shall receive a refund of any prepaid but unused fees for the period following the effective date of termination.

8.5 Where ***Processor*** engages subcontractors, ***Processor*** shall be obliged to pass on ***Processor's*** contractual obligations hereunder to such subcontractors. This shall apply in particular, but shall not be limited to, the contractual requirements for confidentiality, data protection and data security stipulated between the parties of the ***Agreement***.

8.6 Where ***Processer*** engages subcontractors, ***Processor*** shall be deemed to have performed any work or activity, actually performed by a subcontractor, and remain responsible and liable for any work or activities performed by a subcontractor as if ***Processor*** had provided the work or activities itself.

8.7 Where a subcontractor is used, the ***Controller*** must be granted the right to monitor and inspect the subcontractor in accordance with this ***DPA*** (or in accordance with the corresponding provision of the otherwise applicable national data protection law). This also includes the right of the ***Controller*** to obtain information from the ***Processor***, upon written request, on the substance of the contract and the implementation of the data protection obligations within the subcontract relationship, where necessary by inspecting the relevant contract documents.

9 Additional Terms

9.1 Where ***Controller's Personal Data*** becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties while being ***Processed***, ***Processor*** shall inform ***Controller*** without undue delay.

9.2 ***Processor*** shall, without undue delay, notify to all pertinent parties in such action, that any ***Personal Data*** affected thereby is in ***Controller's*** sole property and area of responsibility, that ***Personal Data*** is at ***Controller's*** sole disposition, and that ***Controller*** is the responsible body in the sense of the ***GDPR*** (or a corresponding provision of the otherwise applicable national data protection law).

9.3 With respect to updates and changes to this ***DPA***, the terms that apply in the 'Amendment; No Waiver' section of '***GENERAL TERMS'*** in the ***Agreement*** shall apply.

9.4 In case of any conflict, the regulations of this ***DPA*** shall take precedence over the regulations of the ***Agreement***. Where individual regulations of this ***DPA*** are invalid or unenforceable, the validity and enforceability of the other regulations of this ***DPA*** shall not be affected.

9.5 ***Controller*** will indemnify and hold harmless ***Processor*** against any and all claims from third parties, those of the data protection authority in particular resulting in any way from not complying with this guarantee.

9.6 ***Processor*** guarantees that it will not use ***Customer Data***, which might include ***Personal Data***, which it ***Processes*** in the context of the ***Agreement*** for its own or third party purposes without the ***Controller's*** express written consent, unless legal provisions requires the *Processor* to do so. In such cases ***Processor*** shall immediately inform ***Controller*** of that legal requirement before ***Processing***, unless that law prohibits such information on import grounds of public interest.

9.7 The legal entity agreeing to this ***DPA*** as ***Controller*** represents that it is authorized to agree to and enter into this ***DPA*** for, and is agreeing to this ***DPA*** solely on behalf of, the ***Controller***

Exhibit A. List of Subcontractors

These are the (integrated) ***Subcontractors*** of ***Nebu***, used by ***Nebu*** top provide the ***Nebu Services***:

- **InterMax B.V.** – ***Nebu***'s hosting partner in The Netherlands (www.intermax.nl)
- **CCN GmbH** (Corporate Communications Network) - ***Nebu***'s hosting & telephony provider (BlueSIP) for the DaaS (www.ccn.net & www.bluesip.net)
- **InITova GmbH** – ***Nebu***'s partner for the ***Nebu DaaS*** (www.initova.com)
- **Microsoft Azure - Nebu Data Hub** is using the Azure Platform (www.azure.microsoft.com)
- **RackSpace International GmbH – *Nebu*** is (increasingly) using Rackspace as it hosting management partner (www.rackspace.com)
- **Google Cloud Platform** – ***Nebu*** is using GCP to host part of its applications (www.cloud.google.com/)
- **Dapresy GmbH** – ***Nebu*** is reseller of the Dapresy dashboarding solution under the ***Nebu Dashboards*** label (https://www.dapresy.com)
- **DataExpert Kft – Nebu** often engages DataExpert fort the performance of Professional Services (www.dataexpert.hu)
- **Nebu Hungary Kft.** – the wholly owned subsidiary of ***Nebu B.V.*** in Hungary, mainly focused on the product development and support of the ***Nebu Services***
- Any other wholly-owned ***Nebu B.V.*** subsidiary organizations