

# Nebu Data Processing Agreement

*(DPA)*

<b>Reference</b>	:	Nebu - I-2019 - 0075
<b>Version</b>	:	2.2
<b>Date</b>	:	March 2, 2021
<b>Owner</b>	:	Otto van Linden
<b>Validation:</b>	:	Zoltan Szuhai
<b>Status</b>	:	Final
<b>Qualification</b>	:	Public

**CONTENTS**

1 Introduction ..... 3

2 Definitions ..... 3

3 Scope and Responsibility ..... 5

4 Obligations of Processor ..... 5

5 Obligations of Controller..... 7

6 Enquiries by Data Subjects to Controller ..... 8

7 Audit Obligations ..... 9

8 Subcontractors..... 9

9 Data Transfers..... 10

10 Additional Terms..... 11

Exhibit A. List of Subcontractors ..... 12

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
V2.0	Final	February 16, 2021	Amendments to > Responsibilities of Controller (mainly 5.3, 5.9) > Added Data Transfers (9) > Some definitions added (1) > Amendment to list of Subcontractors (exhibit)
V2.2	Final	March 2, 2021	> Including handling data transfer to third countries in accordance with Standard Contractual Clauses (9.5 & 9.5). Also included in the exhibit.

## 1 Introduction

This Nebu Data Processing Agreement (“**DPA**”) reflects the **Parties’** agreement with respect to the terms governing the **Processing of Personal Data** by **Nebu** on behalf of our **Customers** under the **Nebu General term & Conditions** (the “**Agreement**”). This **DPA** is a supplement to, and forms an integral part of, the **Agreement** and is effective from January 1, 2018, the moment of incorporation into the **Agreement**, which may be specified in the **Agreement**, an **Order** or an executed amendment to the Agreement.

The main purpose 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, hereafter also referred to as **GDPR**)*

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 or 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 acting towards **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) “**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the **Processing of Personal Data**.
- (ii) “**Customer Data**” means all information that **Customer** submits, collects, generates or processes via the **Nebu Services**.
- (iii) “**Data Protection Laws**” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of **Processing Personal Data** in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated or replaced from time to time.
- (iv) “**Data Subject**” means the individual to whom Personal Data relates.
- (v) “**Europe**” means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom
- (vi) “**European Data**” means **Personal Data** that is subject to the protection of **European Data Protection Laws**.

- (vii) “**European Data Protection Laws**” means data protection laws applicable in **Europe**, including: (i) **GDPR**; (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the **GDPR** or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union.
- (viii) “**Personal Data**” means any individual element of information concerning the personal or material circumstances of an identified or identifiable individual.
- (ix) “**Processing**” means processing of **Personal Data** on behalf, encompassing the recording, organization, structuring, storage, adaptation or alteration, retrieval, amendment, consultation, use, disclosure by transmission, transfer, dissemination or otherwise making available, alignment or combination, restriction, blocking or erasure of **Personal Data** by the **Processor** acting on behalf of the **Controller**.
- (x) “**Processor**” means a natural or legal person, public authority, agency or other body which **Processes Personal Data** on behalf of the **Controller**.
- (xi) “**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).
- (xii) “**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.
- (xiii) “**Standard Contractual Clauses**” means the standard contractual clauses for **Processors** established in third countries approved pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010, in the form set out at Annex 3; as may be amended, superseded or replaced.
- (xiv) “**Sub-Processor**” (also referred to as **Subcontractors**) means any **Processor** engaged by **Nebu** or our **Affiliates** to assist in fulfilling our obligations with respect to the provision of the **Nebu Services** under the **Agreement**. **Sub-Processors** may include third parties or our **Affiliates** but will exclude any HubSpot employee or consultant.
- (xv) “**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 or becomes aware that an **Instruction** of the **Controller** infringes any data protection provisions, it shall i) point this out to the **Controller** without delay; and ii) where necessary, cease all **Processing** (other than merely storing and maintaining the security of the affected **Personal Data**) until such time as **Controller** issues new Instructions with which **Processor** is able to comply with. If this provision is invoked, we will not be liable to you under the **Agreement** for any failure to perform the applicable **Nebu Services** until such time as **Controller** issues new lawful **Instructions** regarding the **Processing**.
- 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 reasonably 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 **Data Protection Laws**. Such measures will ensure a level of security appropriate to the risk considering 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).
- 4.5 **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.
- 4.6 Upon **Controller's** request, **Processor** shall provide a current **Personal Data** protection and security programme covering **Processing** hereunder.
- 4.7 **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.
- 4.8 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**.

- 4.9 **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**.
- 4.10 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.
- 4.11 **Processor** shall support **Controller** in fulfilling **Controller's** disclosure obligations under **GDPR** (or a corresponding provision of the otherwise applicable **Data Protection Laws**). To the extent that the required information is reasonably available to **Processor**, and **Controller** do not otherwise have access to the required information, **Processor** will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by (European) **Data Protection Laws**.
- 4.12 **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.
- 4.13 **Processor** shall, upon **Controller's** request, provide to **Controller** all information on **Controller's Customer Data**, which might include **Personal Data**, and information.
- 4.14 **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.
- 4.15 **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 Laws** regulations as are applicable to them.
- 5.2 Within the scope of the **Agreement** and in its use of the **Nebu Services**, the **Controller** will be responsible for complying with all requirements that apply to it under applicable **Data Protection Laws** with respect to its **Processing** of **Personal Data** and the **Instructions** it issues to us.

- 5.3 In particular but without prejudice to the generality of the stated under 5.2, **Controller** acknowledge and agrees that **Controller** will be solely responsible for: (i) the accuracy, quality, and legality of **Customer Data** and the means by which you acquired **Personal Data**; (ii) complying with all necessary transparency and lawfulness requirements under applicable **Data Protection Laws** for the collection and use of the **Personal Data**, including obtaining any necessary consents and authorizations (particularly for use by **Customer** for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the **Personal Data** to us for **Processing** in accordance with the terms of the **Agreement** (including this **DPA**); (iv) ensuring that your Instructions to us regarding the **Processing of Personal Data** comply with applicable laws, including **Data Protection Laws**; and (v) complying with all laws (including **Data Protection Laws**) applicable to any emails or other content created, sent or managed through the **Nebu Services**, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices.
- 5.4 **Controller** shall inform **Processor** without undue delay and comprehensively about any errors, irregularities, or if it is not able to comply with its responsibilities under this sub-section 5.3 or applicable **Data Protection Laws** on the **Processing of Customer Data**, which might include **Personal Data**, detected during a verification of the results of such **Processing**.
- 5.5 **Controller** shall be obliged to maintain the publicly available register or a corresponding provision) of the applicable national data protection law, if any.
- 5.6 **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.
- 5.7 **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.
- 5.8 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**.
- 5.9 The parties agree that the **Agreement** (including this **DPA**), together with your use of the **Nebu Services** in accordance with the **Agreement**, constitute Controller's complete and final **Instructions to Processor** in relation to the **Processing of Personal Data**, and additional instructions outside the scope of the **Instructions** shall require prior written agreement between **Parties**.

## 6 Enquiries by Data Subjects to Controller

- 6.1 The **Nebu Service** provides **Controller** with a number of controls that you can use to retrieve, correct, delete or restrict **Personal Data**, which **Controller** can use to assist it in connection with its obligations under **Data Protection Laws**, including your obligations relating to responding to requests from **Data Subjects** to exercise their rights under applicable **Data Protection Laws** ("Data Subject Requests").



- 6.2 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**, and to the extent that **Controller** is reasonably unable to independently address a **Data Subject Request** through the **Nebu Services, 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 reasonable costs arising from this assistance.
- 6.3 Where a **Data Subject** requests the **Processor** directly 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 (including, where appropriate, the **Standard Contractual Clauses**), to the extent applicable to the nature of the services provided by such **Sub-Processor**, 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 **Processor** 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 *Data Protection Laws*). 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 Data Transfers

- 9.1 **Controller** acknowledge and agree that **Processor** may access and **Process Personal Data** on a global basis as necessary to provide the **Nebu Services** in accordance with the **Agreement**, and in particular that **Personal Data** will be transferred to and **Processed** by Nebu B.V. in the Netherlands and to other jurisdictions where **Nebu Affiliates** and **Sub-Processors** have operations. **Processor** will ensure such transfers are made in compliance with the requirements of **Data Protection Laws**.
- 9.2 **Processor** shall not transfer **European Data** to any country or recipient not recognized as providing an adequate level of protection for **Personal Data** (within the meaning of applicable **European Data Protection Laws**), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable **European Data Protection Laws**. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for **Personal Data**, to a recipient that has achieved binding corporate rules authorization in accordance with **European Data Protection Laws**, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable **European Data Protection Laws**.
- 9.3 As a matter of transparency, **Controller** acknowledges that in connection with the performance of the **Nebu Services**, Nebu B.V. might transfer **Customer Data**, which may include **Personal Data**, to processors in other region than the designated **Data Centre Regions**, as indicated in Exhibit A- List of Subcontractors.

- 9.4 **Parties** acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on **Standard Contractual Clauses** for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the **Controller** (data exporter) may provide a general consent to onward sub-processing by the **Processor**.
- 9.5 Accordingly, the **Controller** mandates the **Processor** to sign Model Clauses 2010/87/EU with their non-EEA-based sub processors in the name and on behalf of the **Controller**. The latter remains the data exporter and the **Sub-processor** is the data importer under those terms. The **Controller** also agrees, in advance, to the content of Appendices 1 and 2 of Model Clauses 2010/87/EU.

## 10 Additional Terms

- 10.1 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.
- 10.2 **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).
- 10.3 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.
- 10.4 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.
- 10.5 **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.
- 10.6 **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.
- 10.7 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** to provide the **Nebu Services**:

Environment	Sub-Processor Link	Country /Region	SCC <sup>5)</sup>	Services											
				Nebu Data Viewer	Nebu Reporter	Nebu DaaS	Nebu Data Hub	Nebu Interviewer	Duo Knowledge	Nebu Panel Manager	Nebu Assessment (Esperto)	Nebu Dashboard (Dapresy)	Nebu Dashboard (Datasmoothie)		
<b>EMEA</b>															
Google Cloud Services	<a href="http://cloud.google.com">cloud.google.com</a>	NL / EMEA	X	X	X					X		X	X		
MS Azure	<a href="http://www.azure.microsoft.com">www.azure.microsoft.com</a>	NL / EMEA	X				X	X					X	X	
AWS	<a href="http://www.aws.com">www.aws.com</a>	NL / EMEA	X							X					
Hetzner	<a href="http://www.hetzner.com">www.hetzner.com</a>	GE / EMEA					X								
<b>North America</b>															
Microsoft Azure	<a href="http://www.azure.microsoft.com">www.azure.microsoft.com</a>	USA / NA		X	X							X		X	
AWS	<a href="http://www.aws.com">www.aws.com</a>	USA / NA								X					
<b>APAC</b>															
MS Azure	<a href="http://www.azure.microsoft.com">www.azure.microsoft.com</a>	SG / APAC		X	X					X			X		
<b>Services</b>															
SendGrid Ltd	<a href="http://www.sendgrid.com">www.sendgrid.com</a>	USA	X	X			X	X							
MailGun Technologies Ltd	<a href="http://www.mailgun.com">www.mailgun.com</a>	USA / GE / BE	X	X						X					
CM ***	<a href="http://www.cm.com">www.cm.com</a>	EMEA		X											
<b>Professional Services</b>															
Rackspace International GmbH	<a href="http://www.rackspace.com">www.rackspace.com</a>	EMEA	X	X	X					X		X	X		
Initova GmbH	<a href="http://www.initova.com">www.initova.com</a>	EMEA					X								
Dapresy GmbH	<a href="http://www.dapresy.com">www.dapresy.com</a>	EMEA & NA												X	
Datasmoothie Ltd	<a href="http://www.datasmoothie.com">www.datasmoothie.com</a>	EMEA												X	
2Gather B.V.*	<a href="http://www.2gather.nl">www.2gather.nl</a>	EMEA		X	X		X	X				X			
Klck B.V. **	<a href="http://www.klck.nl">www.klck.nl</a>	EMEA										X			
Republika -The Research Toolkit GmbH <sup>5)</sup>	<a href="http://www.republika.com">www.republika.com</a>	EMEA								X					
DataExpert Kft ****	<a href="http://www.dataexpert.hu">www.dataexpert.hu</a>	EMEA		X	X		X	X					X		
<b>Affiliates</b>															
Nebu Hungary Kft		EMEA		X	X	X	X	X	X	X	X	X	X	X	
Any other wholly-owned Nebu B.V. subsidiary organizations															

\* 2Gather is our partner in Esperto ([www.espertoassessments.com](http://www.espertoassessments.com))

\*\* Klck, built and managed our Nebu Member Portals

\*\*\* CM provides our SMS-invitation services

\*\*\*\* DataExpert. Our fixed professional services partner

<sup>5)</sup> Our development partner for Nebu Panel Manager

In case of transfer of personal data to **Sub-processors** established in third countries, as indicated in the above table with SCC, under Directive 95/46/EC, **Nebu** has instituted the required security measures by means of a full data processing agreement, which includes the **Standard Contractual Clauses** as per article 9.5.