Customer Data Processing Agreement

Version 2018-05-23

This Customer Data Processing Agreement reflects the requirements of the European Data Protection Regulation (“GDPR”) as it comes into effect on May 25, 2018. Products and services offered in the European Union are GDPR ready and this DPA provides you with the necessary documentation of this readiness.

This Data Processing Agreement (“DPA”) is an addendum to the Customer Terms of Service (“Agreement”)

between

nanocosmos GmbH (“nanocosmos”, “Supplier”)

and

You / the Customer/Licensee.

All capitalized terms not defined in this DPA shall have the meanings set forth in the Agreement. Customer enters into this DPA on behalf of itself and, to the extent required under Data Protection Laws, in the name and on behalf of its Authorized Affiliates (defined below).

The parties agree as follows:

1. Definitions

“Affiliate” means an entity that directly or indirectly Controls, is Controlled by or is under common Control with an entity.

“Authorized Affiliate” means any of Customer Affiliate(s) permitted to or otherwise receiving the benefit of the Services pursuant to the Agreement.

“Control” means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term “Controlled” shall be construed accordingly.

“Controller” means an entity that determines the purposes and means of the processing of Personal Data.

“Customer Data” means any data that Supplier and/or its Affiliates processes on behalf of Customer in the course of providing the Services under the Agreement.

“Data Protection Laws” means all data protection and privacy laws and regulations applicable to the processing of Personal Data under the Agreement, including, where applicable, EU Data Protection Law.

“EU Data Protection Law” means (i) General Data Protection Regulation (“GDPR”), Regulation 2016/679 of the European Parliament; and (ii) Directive 2002/58/EC concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and applicable national implementations of it (in each case, as may be amended, superseded or replaced).

“Personal Data” means any Customer Data relating to an identified or identifiable natural person to the extent that such information is protected as personal data under applicable Data Protection Law.

“Privacy Shield” means the EU-US and Swiss-US Privacy Shield Frameworks, as administered by the U.S. Department of Commerce.

“Privacy Shield Principles” means the Privacy Shield Framework Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of 12 July 2016 pursuant to the Directive, details of which can be found at www.privacyshield.gov/eu-us-framework.

“Processor” means an entity that processes Personal Data on behalf of the Controller.

“Processing” has the meaning given to it in the GDPR and “process”, “processes” and “processed” shall be interpreted accordingly.

“Security Incident” means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data.

“Services” means any product or service provided by Supplier to Customer pursuant to and as more particularly described in the Agreement.

“Sub-processor” means any Processor engaged by Supplier or its Affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the

Agreement or this DPA. Sub-processors may include third parties or any Supplier Affiliate.

2. Scope and Applicability of this DPA

2.1 This DPA applies where and only to the extent that Supplier processes Personal Data on behalf of the Customer in the course of providing the Services and such Personal Data is subject to Data Protection Laws of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom. The parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

2.2 Role of the Parties. As between Supplier and Customer, Customer is the Controller of Personal Data and Supplier shall process Personal Data only as a Processor on behalf of Customer. Nothing in the Agreement or this DPA shall prevent Supplier from using or sharing any data that Supplier would otherwise collect and process independently of Customer's use of the Services.

2.3 Customer Obligations. Customer agrees that (i) it shall comply with its obligations as a Controller under Data Protection Laws in respect of its processing of Personal Data and any processing instructions it issues to Supplier; and (ii) it has provided notice and obtained (or shall obtain) all consents and rights necessary under Data Protection Laws for Supplier to process Personal Data and provide the Services pursuant to the Agreement and this DPA.

2.4 Supplier Processing of Personal Data. As a Processor, Supplier shall process Personal Data only for the following purposes: (i) processing to perform the Services in accordance with the Agreement; (ii) processing to perform any steps necessary for the performance of the Agreement; and (iii) to comply with other reasonable instructions provided by Customer to the extent they are consistent with the terms of this Agreement and only in accordance with Customer’s documented lawful instructions. The parties agree that this DPA and the Agreement set out the Customer’s complete and final instructions to Supplier in relation to the processing of Personal Data and processing outside the scope of these instructions (if any) shall require prior written agreement between Customer and Supplier.

2.5 Nature of the Data. Supplier handles Customer Data provided by Customer. Such Customer Data may contain special categories of data depending on how the Services are used by Customer. The Customer Data may be subject to the following process activities: (i) storage and other processing necessary to provide, maintain and improve

the Services provided to Customer; (ii) to provide customer and technical support to Customer; and (iii) disclosures as required by law or otherwise set forth in the Agreement.

2.6 Supplier Data. Notwithstanding anything to the contrary in the Agreement (including this DPA), Customer acknowledges that Supplier shall have a right to use and disclose data relating to and/or obtained in connection with the operation, support and/or use of the Services for its legitimate business purposes, such as billing, account management, technical support, product development and sales and marketing. To the extent any such data is considered personal data under Data Protection Laws, Supplier is the Controller of such data and accordingly shall process such data in compliance with Data Protection Laws.

3. Subprocessing

3.1 Authorized Sub-processors. Customer agrees that Supplier may engage Sub-processors to process Personal Data on Customer's behalf. The Sub-processors currently engaged by Supplier and authorized by Customer are listed in Annex A.

3.2 Sub-processor Obligations. Supplier shall: (i) enter into a written agreement with the Sub-processor imposing data protection terms that require the Sub-processor to protect the Personal Data to the standard required by Data Protection Laws; and (ii) remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause Supplier to breach any of its obligations under this DPA.

3.3 Changes to Sub-processors. Supplier shall provide Customer reasonable advance notice (for which electronic communication e.g. email shall suffice) if it adds or removes Sub-processors.

3.4 Objection to Sub-processors. Customer may object in writing to Supplier’s appointment of a new Sub-processor on reasonable grounds relating to data protection by notifying Supplier promptly in writing within five (5) calendar days of receipt of Supplier’s notice in accordance with Section 3.3. Such notice shall explain the reasonable grounds for the objection. In such event, the parties shall discuss such concerns in good faith with a view to achieving commercially reasonable resolution. If this is not possible, either party may terminate the applicable Services that cannot be provided by Supplier without the use of the objected-to-new Sub-processor.

4. Security

4.1 Security Measures. Supplier shall implement and maintain appropriate technical and organizational security measures to protect Personal Data from Security Incidents and to preserve the security and confidentiality of the Personal Data, in accordance with Supplier's security standards described in Annex B (“Security Measures”).

4.2 Confidentiality of Processing. Supplier shall ensure that any person who is authorized by Supplier to process Personal Data (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

4.3 Security Incident Response. Upon becoming aware of a Security Incident, Supplier shall notify Customer relating to the Security Incident as it becomes known or as is reasonably requested by Customer.

4.4 Updates to Security Measures. Customer acknowledges that the Security Measures are subject to technical progress and development and that Supplier may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services purchased by the Customer.

5. Security Reports and Audits

5.1 Supplier shall maintain records of its security standards. Supplier shall provide written responses (on a confidential basis) to all reasonable requests for information made by Customer, including responses to information security and audit questionnaires, that Customer (acting reasonably) considers necessary to confirm Supplier's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

5.2 Supplier may assert a claim for remuneration for enabling these inspections.

6. International Transfers

6.1 Processing Locations. Supplier stores and processes EU Data (defined below) in data centers located inside and outside the European Union. All other Customer Data may be transferred and processed in the United States and anywhere in the world where

Customer, its Affiliates and/or its Sub-processors maintain data processing operations. Supplier shall implement appropriate safeguards to protect the Personal Data, wherever it is processed, in accordance with the requirements of Data Protection Laws.

6.2 Transfer Mechanism: Notwithstanding Section 6.1, to the extent Supplier processes or transfers (directly or via onward transfer) Personal Data under this DPA from the European Union, the European Economic Area and/or their member states and Switzerland ("EU Data") in or to countries which do not ensure an adequate level of data protection within the meaning of applicable Data Protection Laws of the foregoing territories, the parties agree that Supplier shall be deemed to provide appropriate safeguards for such data by virtue of having certified its compliance with the Privacy Shield and Supplier shall process such data in compliance with the Privacy Shield Principles. Customer hereby authorises any transfer of EU Data to, or access to EU Data from, such destinations outside the EU subject to any of these measures having been taken.

7. Return or Deletion of Data

7.1 Upon deactivation of the Services, all Personal Data shall be deleted, save that this requirement shall not apply to the extent Supplier is required by applicable law to retain some or all of the Personal Data, or to Personal Data it has archived on back-up systems, which such Personal Data Supplier shall securely isolate and protect from any further processing, except to the extent required by applicable law.

8. Cooperation

8.1 To the extent that Customer is unable to independently access the relevant Personal Data within the Services, Supplier shall (at Customer's expense) taking into account the nature of the processing, provide reasonable cooperation to assist Customer by appropriate technical and organizational measures, in so far as is possible, to respond to any requests from individuals or applicable data protection authorities relating to the processing of Personal Data under the Agreement. In the event that any such request is made directly to Supplier, Supplier shall not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Supplier is required to respond to such a request, Supplier shall promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

8.2 To the extent Supplier is required under Data Protection Law, Supplier shall (at Customer's expense) provide reasonably requested information regarding Supplier's

processing of Personal Data under the Agreement to enable the Customer to carry out data protection impact assessments or prior consultations with data protection authorities as required by law.

9. Miscellaneous

9.1 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

9.2 This DPA is a part of and incorporated into the Agreement so references to "Agreement" in the Agreement shall include this DPA.

9.3 In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise.

9.4 This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

Nanocosmos Informationstechnologien gmbh, Berlin, Germany

Name: Oliver Lietz

Title: CEO/Managing Director

Annex A - List of Supplier Sub-processors

Available upon request

Annex B – Security Measures

Available upon request