Nitro Business Data Processing Addendum

Last Updated: 2022-10-28

TABLE OF CONTENTS

Nitro Business Data Processing Addendum

This Data Processing Addendum ("**DPA**") forms part of the Nitro Business Terms of Service or Nitro Terms of Services, as applicable, governing the use of Nitro's services ("**Agreement**") entered by and between You or the Licensee (each as defined in the relevant Agreement; and for purposes of this DPA, You and Licensee are herein referred to as "**Customer**") and Nitro Software, Inc. ("**Nitro**") to reflect the parties' agreement with regard to the Processing of Personal Data by Nitro solely on behalf of the Customer under the Agreement. Both Parties shall be referred to as the "**Parties**" and each, a "**Party**".

1. DEFINITIONS

For purposes of this DPA, the terms below have the meanings set forth below. Capitalized terms that are used but not defined in this DPA have the meanings given in the Agreement.

(a) **Affiliate** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity, where "control" refers to the power to direct or cause the direction of the subject entity, whether (i) through ownership of voting securities, or (ii) through the ability to in fact control the management decisions of such entity, by contract or otherwise.

(b) **API** means any application programming interface made available by Nitro to the Customer in connection with the Agreement.

(c) **Applicable Data Protection Laws** means the privacy, data protection and data security laws and regulations of any jurisdiction applicable to the Processing of Personal Data under the Agreement, including, without limitation, European Data Protection Laws and the CCPA, each as amended from time to time.

(d) **CCPA** means the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder.

(e) **Customer Data** means information provided or made available to Nitro for Processing on Customer's behalf to perform the Services.

(f) **Documentation** means User Guide, release notes, implementation guides and any other technical documentation related to the Services or Professional Services which is made available to Customer by Nitro.

(g) **EEA** means the European Economic Area.

(h) **European Data Protection Laws** means the GDPR and other data protection laws and regulations of the European Union, its Member States, Switzerland, Iceland, Liechtenstein, Norway and the United

Kingdom, in each case, to the extent applicable to the Processing of Personal Data under the Agreement.

(i) **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as amended from time to time.

(j) **Information Security Incident** means a known breach of Nitro's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data in Nitro's possession, custody or control. Information Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including, but not limited to, unsuccessful log-in attempts, pings, port scans, denial of service attacks, or other network attacks on firewalls or networked systems.

(k) **Intellectual Property Rights** means all intellectual property rights throughout the world, including: (i) patents, disclosures of inventions (whether or not patentable), patent applications, reissues, reexaminations, utility model rights and design rights (registered or otherwise), and registered or other industrial property rights, (ii) trademarks, service marks, corporate names, trade names, Internet identifiers, trade dress, and other similar designations of source or origin together with the goodwill symbolized by any of the foregoing, (iii) copyrights, moral rights, design rights, database rights, data collections, and other sui generis rights, (iv) trade secrets or other proprietary rights in confidential information or technical, regulatory and other information, designs, results, techniques, and other know-how, and (v) applications, registrations, and renewals for, and all associated rights with respect to, any of the foregoing in any part of the world.

(l) **Personal Data** means Customer Data that constitutes "personal data," "personal information," or "personally identifiable information" defined in Applicable Data Protection Law, or information of a similar character regulated thereby, except that Personal Data does not include such information pertaining to Customer's personnel or representatives who are business contacts of Nitro in the normal course of the business relationship, where Nitro acts as a controller of such information.

(m) **Processing** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

(n) **Professional Services** means any services performed by Nitro relating to the Services such as activation, training, configuration, integration, assessment, and optimization.

(o) **Security Measures** has the meaning given in Section 5(a) (Provider's Security Measures).

(p) **Standard Contractual Clauses** means the mandatory provisions of the standard contractual clauses for the transfer of personal data to processors established in third countries in the form set

out by European Commission Decision 2016/679/EU and 2018/914/EU, and implemented by the European Commission decision 2021/914, dated 4 June 2021.

(q) **Sub-processors** means third parties that Nitro engages to Process Personal Data in relation to the Services.

(r) **Third Party Sub-processors** has the meaning given in Section 5 (Sub-processors) of Annex 1.

(s) The terms **controller**, **data subject**, **processor**, and **supervisory authority** as used in this DPA have the meanings given in the GDPR.

2. DURATION AND SCOPE OF DPA

(a) This DPA will remain in effect so long as Nitro processes Personal Data, notwithstanding the expiration or termination of the Agreement.

(b) Annex 1 (EU Annex) to this DPA applies solely to Processing subject to European Data Protection Laws.

(c) Annex 2 (California Annex) to this DPA applies solely to Processing subject to the CCPA if Customer is a "business" or "service provider" (as defined in CCPA) with respect to such Processing.

3. CUSTOMER INSTRUCTIONS

Nitro will process Personal Data only in accordance with Customer's instructions to Nitro. This DPA is a complete expression of such instructions, and Customer's additional instructions will be binding on Nitro only pursuant to an amendment to this DPA signed by both Parties. Customer instructs Nitro to process Personal Data to provide the Services as contemplated by the Agreement.

4. ANALYTICS

Customer acknowledges and agrees that, as a part of the Services, Nitro may:

(a) create and derive from Processing related to the Services elements that are necessary to provide the Services; and/or

(b) create and derive from processing related to the Services anonymized and/or aggregated data that does not identify Customer or any natural person, and use, publicize or share with third parties such anonymized and/or aggregated data to improve Nitro's products and services and/or for its other legitimate business purposes.

5. SECURITY

(a) Provider Security Measures. Nitro will implement and maintain technical and organizational measures designed to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data ("Security Measures") as described in Annex 3 (Security Measures). Nitro may update the Security Measures from time to time without notice, so long as the updated measures do not materially decrease the overall protection of Personal Data.

(b) Information Security Incidents. Nitro will notify Customer without undue delay of any Information Security Incident of which Nitro becomes aware. Such notifications may describe available details of the Information Security Incident, including a summary of steps taken to mitigate the potential risks and steps Nitro recommends Customer consider taking to address the Information Security Incident. Nitro's notification of or response to an Information Security Incident will not be construed as Nitro's acknowledgement of any fault or liability with respect to the Information Security Incident.

(c) Customer's Security Responsibilities and Assessment.

(i) Customer's Security Responsibilities. Customer agrees that, without limitation of Nitro's obligations under Section 5 (Security), Customer is solely responsible for its use of the Services, including (a) making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Personal Data; (b) securing the account authentication credentials, systems and devices Customer uses to access the Services; (c) securing Customer's systems and devices that Nitro uses to provide the Services; and (d) backing up Personal Data.

(ii) Customer's Security Assessment. Customer agrees that the Services, the Security Measures and Nitro's commitments under this DPA are adequate to meet Customer's needs, including with respect to any security obligations of Customer under Applicable Data Protection Laws, and provide a level of security appropriate to the risk in respect of the Personal Data.

6. DATA SUBJECT RIGHTS

(a) Nitro's Data Subject Request Assistance. Nitro will (taking into account the nature of the Processing of Personal Data) provide Customer with assistance reasonably necessary for Customer to perform its obligations under Applicable Data Protection Laws to fulfill requests by data subjects to exercise their rights under Applicable Data Protection Laws ("Data Subject Requests") with respect to Personal Data in Nitro's possession or control. Customer shall compensate Nitro for any such assistance at Nitro's then-current professional services rates, which shall be made available to Customer upon request.

(b) Customer's Responsibility for Requests. If Nitro receives a Data Subject Request, Nitro will advise the data subject to submit the request to Customer and Customer will be responsible for responding to the request.

7. CUSTOMER RESPONSIBILITIES

(a) Customer Compliance. Customer shall comply with its obligations under Applicable Data Protection Laws. Customer shall ensure (and is solely responsible for ensuring) that its instructions in Section 3 comply with Applicable Data Protection Laws, and that Customer has given all notices to, and has obtained all consents from, individuals to whom Personal Data pertains and all other parties as required by Applicable Data Protection Laws for Customer to Process Personal Data as contemplated by the Agreement.

(b) Prohibited Data. Customer represents and warrants to Nitro that Customer Data does not and will not, without Nitro's prior written consent, contain any social security numbers or other government-issued identification numbers; biometric information; passwords for online accounts; credentials to any financial accounts; tax return data; credit reports or consumer reports; any payment card information subject to the Payment Card Industry Data Security Standard; information subject to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act or the regulations promulgated under either such law; information subject to restrictions under Applicable Data Protection Laws governing Personal Data of children, including, without limitation, all information about children under 13 years of age; or any information that falls within any special categories of data (as defined in GDPR). Customer further represents that Customer Data does not and will not contain protected health information subject to the Health Insurance Portability and Accountability Act (HIPAA) or any similar legislation in other jurisdiction; other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or health insurance information unless Customer and Nitro have separately entered into a HIPAA Business Associate Agreement.

8. MISCELLANEOUS

Except as expressly modified by the DPA, the terms of the Agreement remain in full force and effect. In the event of any conflict or inconsistency between this DPA and the terms of the Agreement, this DPA will govern. Notwithstanding anything in the Agreement or any order form entered in connection therewith to the contrary, the Parties acknowledge and agree that Nitro's access to Personal Data does not constitute part of the consideration exchanged by the Parties in respect of the Agreement. Notwithstanding anything to the contrary in the Agreement, any notices required or permitted to be given by Nitro to Customer under this DPA may be given (a) in accordance with any notice clause of the Agreement; (b) to Nitro's primary points of contact at Customer; or (c) to any email provided by Customer for the purpose of providing it with Services-related communications or alerts. Customer is solely responsible for ensuring that such addresses for notifications are valid.

Annex 1 – TO DPA EU ANNEX

1. PROCESSING OF DATA

(a) Subject Matter and Details of Processing. The Parties acknowledge and agree that (i) the subject matter of the Processing under the Agreement is Nitro's provision of the Services; (ii) the duration of the Processing is from Nitro's receipt of Personal Data until deletion of all Personal Data by Nitro in accordance with the Agreement; (iii) the nature and purpose of the Processing is to provide the Services; (iv) the data subjects to whom the Personal Data pertains are Customer (to the extent that Customer is an individual), users of the Services or Nitro's software, and individuals, the Personal Data of whom has been generated, shared or uploaded by Customer and/or users of the Services and/or Nitro's software; and (v) the categories of Personal Data are the personal data generated, shared, uploaded or requested by the Customer or users of the Services and/or Nitro's software (which may include Personal Data contained in documents, pictures and other media and user-generated content such as documents, text, pictures and other content).

(b) Roles and Regulatory Compliance; Authorization. The Parties acknowledge and agree that (i) Nitro is a processor of Personal Data under European Data Protection Laws; (ii) Customer is a controller (or a processor acting on the instructions of a controller) of Personal Data under European Data Protection Laws; and (iii) each Party will comply with the obligations applicable to it in such role under the European Data Protection Laws with respect to the Processing of Personal Data. If Customer is a processor, Customer represents and warrants to Nitro that Customer's instructions and actions with respect to Personal Data, including its appointment of Nitro as another processor, have been authorized by the relevant controller.

(c) Nitro's Compliance with Instructions. Nitro will Process Personal Data only in accordance with Customer's instructions stated in this DPA unless applicable European Data Protection Laws require otherwise, in which case Nitro will notify Customer (unless that law prohibits Nitro from doing so).

(d) Data Deletion. Nitro shall delete all the Personal Data on Nitro's systems on Customer's written request and after the end of the provision of Services, and shall delete existing copies unless continued storage of the Personal Data is required by (i) applicable laws of the European Union or its Member States, with respect to Personal Data subject to European Data Protection Laws or (ii) Applicable Data Protection Laws, with respect to all other Personal Data. Nitro will comply with such instruction as soon as reasonably practicable and no later than 180 days after such expiration or termination, unless Applicable Data Protection Laws require storage. Customer may choose to request a copy of such Personal Data from Nitro for an additional charge by requesting it in writing at least 30 days prior to expiration or termination of the Agreement. Upon the Parties' agreement to such charge pursuant to a work order or other amendment to the Agreement, Nitro will provide such copy of such Personal Data before it is deleted in accordance with this clause.

2. DATA SECURITY

(a) Nitro Security Measures, Controls and Assistance

(i) Nitro Security Assistance. Upon written request, Nitro shall provide Customer with reasonable assistance necessary for Customer to comply with its obligations in respect of Personal Data under European Data Protection Laws, including Articles 32 to 34 (inclusive) of the GDPR, by (a) implementing and maintaining the Security Measures; (b) complying with the terms of Section 5(b) (Information Security Incidents) of the DPA; and (c) complying with this Annex 1. Customer hereby acknowledges and agrees that such measures are sufficient to permit Customer to comply with these obligations.

(ii) Security Compliance by Nitro Staff. Nitro will ensure that its personnel who are authorized to access Personal Data are subject to appropriate confidentiality obligations.3

(b) Reviews and Audits of Compliance Customer may audit Nitro's compliance with its obligations under this DPA no more than once per calendar year and on such other occasions as may be required by European Data Protection Laws, including where mandated by Customer's supervisory authority. Nitro will assist with such audits by providing Customer or Customer's supervisory authority with the information and assistance reasonably necessary to conduct the audit. If a third party is to conduct the audit, Nitro may object to the auditor if the auditor is, in Nitro's reasonable opinion, not independent, a competitor of Nitro, or otherwise manifestly unsuitable. Such objection by Nitro will require Customer to appoint another auditor or conduct the audit itself. To request an audit, Customer must submit a proposed audit plan to Nitro at least three (3) weeks in advance of the proposed audit date and any third party auditor must sign a customary non-disclosure agreement mutually acceptable to Nitro (such acceptance not to be unreasonably withheld) providing for the confidential treatment of all information exchanged in connection with the audit and any reports regarding the results or findings thereof. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. Nitro will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise Nitro security, data protection, privacy, employment or other relevant policies). Nitro will work cooperatively with Customer to agree on a final audit plan. Nothing in this Section 2(b) shall require Nitro to breach any duties of confidentiality. If the controls or measures to be assessed in the requested audit are addressed in an SOC 2 Type 2, ISO, or similar audit report performed by a qualified third party auditor completed within twelve (12) months of Customer's audit request and Nitro has confirmed there have been no known material adverse changes in the controls audited since the date of such report, Customer agrees to accept such report in lieu of requesting an audit of such controls or measures. The audit must be conducted during Nitro's regular business hours, subject to the agreed final audit plan and Nitro's safety, security and/or other relevant policies, and may not unreasonably interfere with Nitro's business activities. Customer will promptly notify Nitro of any non-compliance discovered during the course of an audit and provide Nitro any audit reports generated in connection with any audit under this Section 2(b), unless prohibited by European Data Protection Laws or otherwise instructed by a supervisory authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. Any audits are at Customer's sole expense. Customer shall reimburse Nitro for any time expended by Nitro and any third parties in connection with any audits or inspections under this Section 2(b) at Nitro's then-current professional services rates, which shall be made available to Customer upon request.

Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

3. IMPACT ASSESSMENTS AND CONSULTATIONS

Nitro will (taking into account the nature of the Processing and the information available to Nitro) reasonably assist Customer in complying with its obligations under Articles 35 and 36 of the GDPR, by (a) making available documentation describing relevant aspects of Nitro's information security program and the security measures applied in connection therewith and (b) providing the other information contained in the Agreement, including this DPA.

The Customer confirms those data subjects will by default be considered one of the following categories:

- Customer's staff
- Customer's customers
- Customer's prospects
- Customer's suppliers

4. DATA TRANSFERS

(a) Data Processing Facilities. Nitro may, subject to Section 4(b) (Transfers out of the EEA), store and Process Personal Data in the United States or anywhere Nitro or its Sub-processors maintain facilities.

(b) Transfers out of the EEA. If Customer transfers Personal Data out of the EEA to Nitro in a country not deemed by the European Commission to have adequate data protection, such transfer will be governed by the Standard Contractual Clauses, the terms of which are hereby incorporated into this DPA. In furtherance of the foregoing, the Parties agree that (i) Customer will act as the data exporter and Nitro will act as the data importer under the Standard Contractual Clauses; (ii) for purposes of Appendix 1 to the Standard Contractual Clauses, the categories of data subjects, data, special categories of data (if appropriate), and the Processing operations shall be as set out in Section 1(a) to this Annex 1 (Subject Matter and Details of Processing); (iii) for purposes of Appendix 2 to the Standard Contractual Clauses, the technical and organizational measures shall be the Security Measures; (iv) data importer will provide the copies of the sub-processor agreements that must be sent by the data importer to the data exporter pursuant to Clause 5(j) of the Standard Contractual Clauses upon data exporter's request, and that data importer may remove or redact all commercial information or clauses unrelated the Standard Contractual Clauses or their equivalent beforehand; (v) the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be performed in accordance with Section 2(b) of this Annex 1 (Reviews and Audits of Compliance); (vi) Customer's authorizations in Section 5 (Sub-processors) of this Annex 1 will constitute Customer's prior written consent to the subcontracting by Nitro of the Processing of Personal Data if such consent is required under Clause 5(h) of the Standard Contractual Clauses; and (vii) certification of deletion of Personal Data as described in Clause 12(1) of the Standard Contractual Clauses shall be provided upon data importer's written request.

Notwithstanding the foregoing, the Standard Contractual Clauses (or obligations the same as those under the Standard Contractual Clauses) will not apply to the extent an alternative recognized compliance standard for the transfer of Personal Data outside the EEA in accordance with European Data Protection Laws applies to the transfer. In the event of any conflict or inconsistency between (a) this Annex 1 and any other provision of this DPA, this Annex 1 will govern, or (b) the Standard Contractual Clauses and any other provision of this Agreement, the Standard Contractual Clauses will govern.

5. SUB-PROCESSORS

(a) Consent to Sub-processor Engagement. Customer specifically authorizes the engagement of Nitro's Affiliates as Sub-processors and generally authorizes the engagement of other third parties as Sub-processors ("Third Party Sub-processors").

(b) Information about Sub-processors. Information about Sub-processors, including their functions and locations, is available at: https://www.gonitro.com/trust-center-data-protection/subprocessors-and-subcontractors (as may be updated by Nitro from time to time) or such other website address as Nitro may provide to Customer from time to time (together, "Sub-processor Site").

(c) Requirements for Sub-processor Engagement. When engaging any Sub-processor, Nitro will enter into a written contract with such Sub-processor containing data protection obligations not less protective than those in this DPA with respect to Personal Data to the extent applicable to the nature of the services provided by such Sub-processor. Nitro shall be liable for all obligations under the Agreement subcontracted to, the Sub-processor or its actions and omissions related thereto.

(d) Opportunity to Object to Sub-processor Changes. When Nitro engages any new Third Party Sub-processor after the effective date of the Agreement, Nitro will notify Customer of the engagement (including the name and location of the relevant Sub-processor and the activities it will perform) by updating the Sub-processor Site or by other written means. If Customer objects to such engagement in a written notice to Nitro within 15 days after being informed of the engagement on reasonable grounds relating to the protection of Personal Data, Customer and Nitro will work together in good faith to find a mutually acceptable resolution to address such objection. If the Parties are unable to reach a mutually acceptable resolution within a reasonable timeframe, Customer may, as its sole and exclusive remedy, terminate the Agreement and cancel the Services by providing written notice to Nitro and pay Nitro for all amounts due and owing under the Agreement as of the date of such termination.

(e) Sufficiency of Consent. Customer hereby acknowledges and agrees that the foregoing procedures are sufficient to obtain Customer's prior written consent to the sub-processing under Article 28 of the GDPR, and to the extent required under Clause 5(h) of the Standard Contractual Clauses.

ANNEX 2 TO DPA CALIFORNIA ANNEX

1. For purposes of this Annex 2, the terms “business,” “commercial purpose,” “sell” and “service provider” shall have the respective meanings given thereto in the CCPA, and “personal information” shall mean Personal Data that constitutes personal information governed by the CCPA.

2. It is the Parties’ intent that with respect to any personal information, Nitro is a service provider. Nitro shall not (a) sell any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Services; or (c) retain, use or disclose the personal information outside of the direct business relationship between Nitro and Customer. Nitro hereby certifies that it understands its obligations under this Section 2 and will comply with them.

3. The Parties acknowledge that Nitro’s retention, use and disclosure of personal information authorized by Customer’s instructions documented in the DPA are integral to Nitro’s provision of the Services and the business relationship between the Parties.

ANNEX 3 TO DPA SECURITY MEASURES

The protection of information is the main purpose of information security, which is achieved by implementing a suitable set of controls, including organizational structures, policies and procedures, processes, and technical IT controls. These controls need to be designed, implemented, monitored, reviewed, and improved to ensure that the information assets of Nitro and its Affiliates, its partners or customers are secure at all times. Refer to Technical Organizational Measures