cadence®

DATA PROCESSING AGREEMENT

Cadence Design Systems, Inc., having offices at 2655 Seely Avenue, San Jose, California 95134, USA ("**Cadence**"), and the Vendor identified below ("**Vendor**"), hereby agree to this Data Processing Agreement ("**DPA**"), effective as of the last signature hereto ("**Effective Date**"). This DPA forms an integral part of the separate commercial agreement(s) between Vendor and Cadence (together, the "**Parties**") that pertains to the purchase by Cadence of products and/or services from Vendor ("**Commercial Agreement**"). The Parties enter into this DPA on behalf of themselves and their Affiliates.

1. ORDER OF PRECEDENCE; SURVIVAL.

Terms not defined in this DPA or in applicable Data Protection Legislation, shall have the meaning assigned to them in the Commercial Agreement. In the event of any conflict or inconsistency, this DPA shall supersede and prevail over any conflicting terms in the Commercial Agreement. The provisions of this DPA shall survive any termination of the Commercial Agreement.

2. DEFINITIONS.

2.1. "**Affiliate**" means any entity under the control of a party where "control" means ownership of or the right to control greater than fifty percent (50%) of the voting securities of such entity, or equivalent.

2.2. "**Aggregate Data**" means a compilation of data that relates to a group or category of individuals, from which Personal Data has been removed, and is not linked or reasonably linkable to any Personal Data.

2.3. "**Cadence Data**" means Personal Data that is directly or indirectly supplied by Cadence to the Vendor under the applicable Commercial Agreement or which the Vendor is required to process pursuant to the Commercial Agreement.

2.4. "**Data Protection Legislation**" means, to the extent applicable:

2.4.1. The EU Data Protection Directive 95/46/EC, as transposed into EU Member State law, and any amending or replacement legislation, including the May 25th 2018 Regulation (EU) 2016/679 ("**GDPR**"), as well as any EU Member State laws enacted in conjunction with the GDPR.

2.4.2. All applicable laws and regulations, worldwide (whether, national, state, provincial, local or otherwise), relating to the access, use, protection, disclosure, processing, security, privacy, and/or confidentiality of Personal Data, as may be amended, extended, re-enacted, or interpreted from time-to-time and including without limitation, any applicable jurisdiction-specific terms specified in Addendum B.

2.5. "**Personal Data**" means any and all individually or personally identifiable information of or about, or that relates to, describes, is reasonably capable of being associated with, or could reasonably be linked directly or indirectly with, a data subject, or of or about any other individuals that Vendor or any Vendor Party has access to, receives, obtains, collects, generates or processes in connection with the provision of products, services, functions, or transactions under this DPA, including without limitation any and all data that falls within the scope of personal data, personal information, individually identifiable information, or any equivalent term as defined by applicable Data Protection Legislation. Personal Data includes, but is not limited to, a data subject's name, address, telephone number, work status, work location, department code, position level, birth date, gender code, hire date, job title, and medical information and protected health information.

2.6. "**Sensitive Data**" means a class of Personal Data including (a) social security number, passport number, driver's license number, or similar identifier, (b) credit or debit card number (other than truncated digits), financial information, banking account numbers or passwords, (c) employment, financial, genetic, biometric or health information, (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation, (e) account passwords, (f) criminal history, or (g) any other information or combinations of information that falls within the definition of "special categories of data" under GDPR or any other applicable Data Protection Legislation. Vendor shall not process or transfer any Sensitive Data unless specifically agreed to by Cadence.

2.7. "**Data Processing Operations**" may include without limitation: delivery of learning, performance, recruiting, onboarding, analytics, succession activities; implementation services; product support; technical, commercial, marketing, legal and/or other projects.

3. DETAILS OF THE PROCESSING.

3.1. Nature and purpose. Vendor will only process the Cadence Data as necessary to perform its obligations under the Commercial Agreement and as further instructed by Cadence in writing.

3.2. Duration. The processing hereunder shall occur on or after the Effective Date until the termination or expiration of the Commercial Agreement, or as otherwise agreed-upon in writing.

3.3. Categories of Data Subjects. Cadence may provide Vendor with Personal Data, which may include without limitation, Personal Data relating to the following categories of data subjects: consumers or users of goods and/or services provided, administered, or operated by Cadence or any Cadence Affiliate; Cadence personnel; and/or third parties that have, or may have, a commercial relationship with Cadence (e.g., advertisers, customers, prospects, business partners, and/or content providers).

3.4. Types of Personal Data. Cadence may provide Vendor with Personal Data generated, shared, uploaded, collected from, or provided by consumers or users of goods and services provided, administered, or operated by Cadence or any Cadence Affiliate; Personal Data of Cadence personnel generated in the normal course of staff administration, e.g., routine employee data; and/or the Personal Data relating to external third parties with whom Cadence has, or may develop, a commercial relationship (e.g., advertisers, customers, prospects, business partners, and/or content providers).

3.5. Classification of the Parties. To the extent that Vendor processes Cadence Data, Vendor is deemed a Processor (as that term is defined in the GDPR or as defined in substantially-equivalent terms in other applicable Data Protection Legislation). For the purposes of this DPA and the Commercial Agreement, Cadence is deemed a Controller (as that term is defined in the GDPR or as defined in substantially-equivalent terms in other applicable Data Protection Legislation).

4. COMPLIANCE.

4.1. Duration. The data processing obligations set out in this DPA shall apply from the Effective Date to Vendor with respect to its Data Processing Operations of Cadence Data. To the extent applicable, the Parties agree to incorporate the data processing obligations set out in the following sections into any future agreements between them.

4.2. Obligations. With respect to any Cadence Data that is processed by Vendor for the purpose of fulfilling Vendor's obligations to Cadence under the Commercial Agreement, Vendor shall:

4.2.1. Comply with all applicable Data Protection Legislation;

4.2.2. Subject to the clause below, only process (e.g., receive, retain, use, sell, transfer, disclose, etc.) Cadence Data pursuant to the specific purpose(s) described in and/or contemplated by the Commercial Agreement, and only in accordance with instructions contained in that Commercial Agreement, or as otherwise received from Cadence in writing; and

4.2.3. Where Vendor is obliged by applicable law to process any Cadence Data that is Personal Data other than in accordance with Section 4.2.2 above, and unless Vendor is otherwise prohibited under applicable law from informing Cadence of such processing, Vendor must inform Cadence of that obligation, providing: (i) as much advance notice of any such processing as is reasonably possible; (ii) a description of the nature and timing of any such processing; and, (iii) details of the applicable law that requires such processing.

5. ACCESS REQUESTS.

5.1. Data Subjects. Insofar as is possible, Vendor shall provide, at no additional cost to Cadence, any resources and assistance reasonably requested by Cadence in order to allow Cadence to comply with

its obligations to data subjects (or equivalent) who exercise their rights under the Data Protection Legislation.

5.2. Assistance. Taking into account the nature of the processing and the information available to Vendor, Vendor shall provide, at no additional cost to Cadence, any resources and assistance reasonably requested by Cadence in order to allow Cadence to comply with its obligations under Articles 32 to 36 of the GDPR (or other applicable Data Protection Legislation), including assisting Cadence with the performance of any relevant data protection impact assessments.

5.3. Audits. Without prejudice to Cadence's rights in the Commercial Agreement, provide such assistance and information as Cadence reasonably requires in order to demonstrate Vendor's compliance with these obligations and permit Cadence or its external advisers and representatives (subject to reasonable notice) to inspect and audit the data processing activities carried out by Vendor, including access to the premises, records, and personnel of Vendor (or Vendor's contractors).

5.4. Infringement. Vendor shall inform Cadence immediately, if, in the Vendor's reasonable opinion, any instruction from Cadence infringes the Data Protection Legislation.

5.5. Records. Vendor shall maintain records as required under certain Data Protection Legislation of all processing activities carried out pursuant to the Commercial Agreement and make such records available to Cadence or its representatives on reasonable demand and notice.

5.6. Notification. Vendor shall notify Cadence immediately if Vendor receives any investigation, communication, inspection, audit, administrative sanction, or fine, from any authority, or any claim, proceedings or complaint by a data subject, which relates directly or indirectly to the processing of Cadence Data under the Commercial Agreement.

6. INCIDENT MANAGEMENT AND NOTIFICATION.

6.1. Notice. In relation to any breach involving Cadence Data, Vendor shall notify Cadence without undue delay (and in any event within forty eight (48) hours) of the discovery by Vendor of any actual or suspected data breach involving Cadence Data, whether or not such a breach is the responsibility of Vendor. Such notice shall include, at the time of notification or as soon as possible after notification, details of the nature of the breach and number of records affected, the category and approximate number of affected data subjects, anticipated consequences of the breach and any actual or proposed remedies for mitigating the possible adverse effects of the breach.

6.2. Assistance. Vendor shall provide Cadence with all resources and assistance as are required by Cadence for it to investigate a breach and enable Cadence to notify the relevant regulatory body (or bodies) and/or the relevant data subjects of such a breach, as applicable.

7. SECURITY.

7.1. Controls. Vendor shall ensure and maintain appropriate, adequate, and reasonable security procedures and practices, and take technical and organizational measures to protect Cadence Data from a confirmed or reasonably suspected accidental or unlawful use, access, destruction, damage, alteration, or disclosure of Cadence Data. Such procedures and practices shall not materially decrease throughout Vendor's access to and processing of Cadence Data.

7.2. Access Requests. At Cadence's request, Vendor will promptly provide a written description of such reasonable security procedures and practices, and technical and organizational measures employed by Vendor for processing Cadence Data. These measures shall be appropriate to the level of risk presented by the processing, appropriate to the nature of the Cadence Data, and to the harm which might result from a personal data breach affecting the Cadence Data.

8. CONFIDENTIALITY.

8.1. Personnel. Vendor shall ensure that only those employees, staff, workers, agents, and consultants of Vendor (and of any Vendor sub-contractor) that need to know, or need to have access, have access to the Cadence Data and that they are under confidentiality obligations with respect to Cadence Data.

Such confidentiality obligations shall include, at a minimum, receiving appropriate training on their data protection responsibilities and executing written confidentiality agreements that survive the termination of the person's engagement.

8.2. Statements. Unless required by applicable law, the Vendor shall not make any statement (or provide any documents) about matters concerning the Commercial Agreement, or the processing of the Cadence Data under the Commercial Agreement, without the written approval of Cadence. Where Vendor is required under applicable law to make any such statement (or provide any documents), Vendor shall first provide to Cadence a copy of any such statements (or documents), unless prohibited by applicable law, and shall co-operate with, and take account of any comments of Cadence prior to such legally required disclosure.

9. RETURN AND DELETION OF CADENCE DATA.

9.1. Requests. Upon written request from Cadence, Vendor shall promptly (but in any event not later than thirty (30) calendar days) delete any particular or all Cadence Data in its possession and certify in writing to Cadence that it has complied with the requirements of this section, provided that, if Vendor is required to maintain any Cadence Data by law, or by the terms of a separate agreement with Cadence, Vendor shall not be required to comply with the deletion requirements of this section, but shall instead provide a written statement to Cadence that identifies the Personal Data that was not deleted and the reason for the non-deletion. Without limiting the foregoing, Vendor may retain Aggregated Data in accordance with the Vendor's standard data retention policies.

9.2. Termination. Without prejudice to Cadence's rights in the Commercial Agreement, at the choice of Cadence, Vendor shall delete, destroy, or return all Cadence Data to Cadence after the termination or expiration of the Commercial Agreement.

10. SUB-PROCESSORS.

10.1. Consent. Vendor shall not subcontract or otherwise engage any sub-processor to carry out processing activities with respect to the Cadence Data ("**Sub-Processor**") without the prior written consent of Cadence, which shall not be unreasonably withheld and which may be conferred in the Commercial Agreement.

10.2. Requirements. Where use of a Sub-Processor has been approved by Cadence, Vendor shall:

10.2.1. Ensure that it enters into a written contract with the Sub-Processor which imposes on each party obligations at least equivalent to and no less protective than those imposed in this DPA.

10.2.2. Ensure that each Sub-Processor complies with their equivalent terms and with Data Protection Legislation.

10.2.3. Unless otherwise specified in the Commercial Agreement, remain fully liable to Cadence for the acts and omissions of its Sub-Processors to the same extent Vendor would be liable under the terms of this DPA.

11. INTERNATIONAL TRANSFERS.

Vendor shall ensure that any international transfers of Personal Data comply with applicable Data Protection Legislation. In the event that Cadence Data is transferred from the European Economic Area, the United Kingdom, and/or Switzerland to outside the European Economic Area, the United Kingdom, and/or Switzerland, either directly or via onward transfer, to any country or recipient not recognized by the European Commission as providing an adequate level of protection for personal data or not covered by Vendor's Binding Corporate Rules, then the Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision 2010/593/EU, as referenced and amended in Addendum A, shall also apply.

12. ADDITIONAL TERMS.

To the extent that Vendor processes the Personal Data of residents listed in one of the jurisdictions specified in Addendum B, then the corresponding additional terms shall apply. In the event of a conflict between Addendum B and any other terms, then the applicable Addendum B terms shall govern.

13. CERTIFICATION.

Vendor certifies that it understands the restrictions in this DPA and will comply with these provisions.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

VENDOR: _____	**CADENCE DESIGN SYSTEMS, INC.**
Signature: _____	**Signature**: Karna Nisewaner (Nov 23, 2020 15:47 PST)
Name: _____	**Name**: Karna Nisewaner
Title: _____	**Title:** VP and Deputy General Counsel
Date: _____	**Date**: Nov 23, 2020

ADDENDUM A: INTERNATIONAL TRANSFERS

The Standard Contractual Clauses for international data transfers[1] ("**SCC**"), shall apply in respect of any Personal Data provided by Cadence to Vendor and/or acquired by Vendor at Cadence's request in connection with the Commercial Agreement. The SCC are construed, amended, and supplemented as follows, and as supplemented by the Commercial Agreement:

A. Appendix 1 to the SCC (describing additional information regarding activities, data subjects, categories of data, and processing operations relating to the transfer) shall include the following:

Data Exporter (Cadence). The Data Exporter uses employee, customer and supplier personal data for business and employment purposes, including without limitation: (1) maintaining and supporting its products and services and complying with its contractual and compliance obligations related thereto; (2) managing employees and customers; (3) satisfying governmental reporting and tax requirements; (4) implementing and maintaining Cadence's information technology; and (5) for other employment-related and business-related purposes permitted or required under applicable local law and regulation.

Data Importer (Vendor). The Data Importer is processing Personal Data so as to perform contractual obligations as a provider of goods or services to the Data Exporter.

B. Appendix 2 to the SCC (describing security measures to be applied by Data Importer) shall consist of the following:

Access Control to Processing Areas and Systems. Data Importer implements suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the personal data are processed or used. These include:

- Securing the data processing equipment;
- Establishing access authorizations for staff and third parties;
- Securing the data center where personal data are hosted by a security alarm system, and other appropriate security measures;
- Automatic time-out of user terminal if left idle, identification and password required to reopen;
- Staff policies in respect of each staff access rights to data, informing staff about their obligations and the consequences of any violations of such obligations, to ensure that staff will only access personal data and resources required to perform their job duties and training of staff on applicable privacy duties and liabilities;
- All access to data content is logged, monitored, and tracked; and
- Use of state of the art encryption technologies.

Transmission Control. Data Importer implements suitable measures to prevent the personal data from used by unauthorized parties. This includes:

- Use of state-of-the-art firewall and encryption technologies to protect the gateways and networks through which the data travels; and
- As far as possible, logging, monitoring, and tracking all data transmissions.

Input Control. Data Importer implements suitable measures to ensure that it is possible to check by whom personal data have been input into data processing systems or removed. This includes:

- Individual authentication credentials such as user ID and passwords;
- Providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are capable of being locked; and
- Automatic log-off of user ID's that have not been used for a substantial period of time.

Job Control. Data Importer implements suitable measures to monitor its system administrators and to ensure that they act in accordance with instructions received. This includes:

- Adoption of suitable measures to register system administrators' access logs and keep them secure and accurate.

[1] As shown on pages 6 to 14 of the document at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF.

Availability Control. Data Importer implements suitable measures to ensure that personal data are protected from accidental destruction or loss. This includes:

- Recording any detected security incident following data recovery procedures, and identifying the person who carried out data recovery procedures; and
- Monitoring system administrators and to ensure that they act in accordance with instructions received.

C. Appendix 3 (describing GDPR requirements) to the SCC shall consist of the following:

Data Importer and sub-processor shall comply with all requirements that the General Data Protection Regulation 2016/679 (GDPR) imposes on data processors and are collectively referred to as "processor" in this Appendix 3. Without limiting provisions elsewhere in this DPA, Data Importer agrees, warrants and represents that it:

a) Processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject. In such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Also, the processor shall immediately inform the controller if, in its opinion, an instruction infringes the GDPR, national data protection laws in the EU or other applicable law;

b) Ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c) Takes all measures required pursuant to Article 32 of the GDPR (security of processing);

d) Respects the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR for engaging another processor;

e) Taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR, including, without limitation, right to access, rectification, erasure and portability of the data subject's personal data; (for the avoidance of doubt, processor shall only assist and enable controller to meet controllers obligations to satisfy data subjects' rights, but processor shall not respond directly to data subjects);

f) Assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR (Security of personal data) taking into account the nature of processing and the information available to the processor;

g) At the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

h) Makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller;

i) Provides notification as required by the GDPR and any other applicable law regarding any loss or breach of security of the personal data;

j) Complies with this Appendix 3, the GDPR and applicable law until termination of services and upon termination, at controller's choice: (1) destroy all personal data processed and any copies thereof and certify to controller on request having done so; or (2) return all data and copies thereof to controller; and

k) Monitors and self-audits its own compliance with its obligations under applicable national data protection law and the GDPR and provide controller with periodic reports, at least annually.

ADDENDUM B: ADDITIONAL TERMS

To the extent that Vendor processes the Personal Information of a resident located in any of the jurisdictions listed below, then the corresponding additional terms shall apply.

1. **Australia.** "Data Protection Legislation" includes the Australian Privacy Principles and the Australian Privacy Act (1988), which shall modify the definitions in the DPA as follows:

   a. The definition of "personal data" includes "Personal Information"; and

   b. The definition of "sensitive data" includes "Sensitive Information."

2. **Brazil.** "Data Protection Legislation" includes the Lei Geral de Proteção de Dados, which shall modify the definitions in the DPA as follows:

   a. The definition of "Security Incident" includes a security incident that may result in any relevant risk or damage to the data subjects; and

   b. The definition of "processor" includes "operator."

3. **California.** "Data Protection Legislation" includes the California Consumer Privacy Act ("CCPA"), which shall modify the definitions in the DPA as follows:

   a. The definition of "personal data" includes "Personal Information";

   b. The definition of "data subject" includes "Consumer";

   c. The definition of "controller" includes "Business"; and

   d. The definition of "processor" includes "Service Provider".

   Vendor will process, retain, use, and disclose personal data only as necessary to provide the Services under the Agreement, which constitutes a business purpose.

   Vendor agrees not to (a) sell (as defined by the CCPA) Cadence Personal Data or Cadence end users' Personal Data, (b) retain, use, or disclose Customer's Personal Data for any commercial purpose (as defined by the CCPA) other than providing the Services, or (c) retain, use, or disclose Customer's personal data outside of the scope of the Agreement.

   Vendor certifies that its Sub-Processors are Service Providers under the CCPA.

4. **Canada.** "Data Protection Legislation" includes the Federal Personal Information Protection and Electronic Documents Act, which shall modify the definition in the DPA as follows:

   a. "Sub-processors" are deemed "third parties," with whom Vendor has entered into a written contract that includes terms substantially similar to this Addendum.

   Vendor has conducted appropriate due diligence on its Sub-processors (or third parties, as the case may be).

   Vendor will implement technical and organizational measures as set forth in this Addendum.

5. **China.** "Data Protection Legislation" includes the Cybersecurity Law.

6. **Israel.** "Data Protection Legislation" includes the Protection of Privacy Law, which shall modify the definitions in the DPA as follows:

   a. The definition of "controller" includes "Database Owner"; and

   b. The definition of "processor" includes "Holder".

   Vendor will require that any personnel authorized to process Cadence Data comply with the principle of data secrecy and have been duly instructed about Data Protection Legislation.

7. **India**. "Data Protection Legislation" includes the Personal Data Protection Bill and The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

8. **Japan.** "Data Protection Legislation" includes the Act on the Protection of Personal Information, which shall modify the definitions in the DPA as follows:

   a. The definition of "personal data" includes "Personal Information";

   b. The definition of "controller" includes "Business Operator"; and

   c. The definition of "processor" includes a business operator entrusted by the Business Operator with the handling of personal data in whole or in part (also a "**trustee**"). As a trustee, Vendor will ensure that the use of the entrusted personal data is securely controlled.

9. **Malaysia.** "Data Protection Legislation" includes the Malaysian Personal Data Protection Act of 2010.

10. **Mexico**. "Data Protection Legislation" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations.

11. **Russia.** "Data Protection Legislation" includes the Data Protection Act.

12. **Singapore.** "Data Protection Legislation" includes the Personal Data Protection Act 2012. Vendor will process personal data to a standard of protection in accordance with the Data Protection Legislation.

13. **South Africa.** "Data Protection Legislation" includes the Protection of Personal Information Act.

14. **South Korea.** "Data Protection Legislation" includes the Personal Information Protection Act.

15. **Taiwan.** "Data Protection Legislation" includes the Personal Data Protection Act.

16. **Thailand.** "Data Protection Legislation" includes the Thailand Personal Data Protection Act.