cadence®

DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") forms an integral part of the separate commercial agreement(s) between Vendor and Cadence, each on behalf of themselves and their Affiliates (together, the "**Parties**") that pertains to the purchase by Cadence of products and/or services from Vendor ("**Commercial Agreement**"). This DPA governs the processing of any personal information that Cadence may make accessible to Vendor and is effective as of the last signature hereto ("**Effective Date**").

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 an entity that now or hereafter controls, is controlled by or is under common control with a specified entity, where "control" means beneficial ownership, directly or indirectly, of more than fifty percent (50%) of the outstanding shares or other ownership interest (representing the right to vote for the election of directors or other managing authority or the right to make the decisions for such entity, as applicable) of an entity. Such entity shall be deemed to be an Affiliate only so long as such control exists.

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 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.

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

2.5.1. 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.

2.5.2. All applicable laws and regulations, binding guidance and/or codes of practices issued by a compentent supervisory authority (including the European Data Protection Board), 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.

2.6. "**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.

2.7. "**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.

2.8. "**Services**" means the products and/or services provided by Vendor to Cadence pursuant to the Commercial Agreement.

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 under the Data Protection Legislation, including to data subjects (or equivalent) who exercise their rights under the Data Protection Legislation. The Vendor shall immediately notify Cadence upon receipt of any request by a data subject to exercise his or her rights under the GDPR (or other applicable Data Protection Legislation) in respect of any Cadence Data (and in any event within two (2) Business Days of becoming aware).

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) (or any relevant regulatory body) 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. The notification to Cadence must include at least the information referred to in Article 33(3) of the GDPR and (to the extent that it is known at the time of notification, with the remainder of such information to be provided as it becomes available) include: (a) a description of the nature of the breach, including where possible the categories, approximate number of data subjects concerned and the identity of each data subject affected; (b) the name and contact details of the Vendor contact from whom more information can be obtained; (c) a description of the measures taken or proposed to be taken to address the breach, including, where appropriate, measures to mitigate its possible adverse effects; and (d) any other information Cadence reasonably requests relating to the breach, to allow Cadence to meet any reporting obligations or inform data subjects of the breach under the Data Protection Legislation.

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 and shall adhere to the minimum standards specified in Addendum C.

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) return all Cadence Data transferred and any copies to Cadence or 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 return and/or 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. In that case, the Vendor shall hold such Cadence Data in accordance with its obligations under this Agreement, and shall not process such Cadence Data for any purpose other than as required by law. 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 or Switzerland to outside the European Economic Area 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 approved by the European Commission in Decision 2021/914/EU (the "**SCCs**"), as referenced and amended in Addendum A, shall also apply. Where a Sub-Processor located outside the EEA is unable to provide a standard of data protection compliance commensurate with that set out in the GDPR, the Vendor shall cease transferring Personal Data to such Sub-Processor immediately and, if necessary, shall procure at its own cost an alternative Sub-Processor. To the extent the SCCs apply to data transfers, the SCCs shall prevail in case there is any conflict between this DPA and/or the Commercial Agreement and the terms of the SCCs.

12. ADDITIONAL TERMS.

To the extent that Vendor processes the Personal Data of residents listed in any 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. UPDATES.

Cadence may update this DPA from time-to-time in order to reflect changes in applicable Data Protection Legislation. An updated copy shall be made publicly available on a www.cadence.com page.

14. 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**: Caroline M. Reebs
Name: _____	**Name**: Caroline M. Reebs
Title: _____	**Title:** Group Director & Lead Counsel
Date: _____	**Date**: November 30, 2022

ADDENDUM A: INTERNATIONAL TRANSFERS

If and to the extent that the Commercial Agreement involves the provision of Services where Vendor will transfer the Cadence Data from any country in the European Economic Area or Switzerland (together, the "**Jurisdiction**") to outside the Jurisdiction, then the parties agrees that the Standard Contractual Clauses approved by the European Commission in Decision 2021/914/EU (the "**SCCs**") shall apply. Should the European Commission annul the Adequacy Decision for Switzerland then the SCCs shall also apply to transfers from the European Union to Switzerland. Please find the full text here: https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf. The SCCs are construed, and/or supplemented as follows:

A. APPLICABLE MODULE

Based on the nature of the Services, the module indicated below shall apply:

- ☐ Module One (Controller to Controller)
- **X** Module Two (Controller to Processor)
- ☐ Module Three (Processor to Processor)
- ☐ Module Four (Processor to Controller)

B. OPTIONS

For each module, where applicable, the Parties agree on the following options:

1. **Clause 7:** the optional docking clause shall apply.
2. **Clause 9(a):** Option 2 applies. Vendor shall: (i) provide as much notice as possible; (ii) take commercially reasonable efforts to ensure that the sub-processor is not a direct competitor of Cadence; and (iii) thereafter provide Cadence with 30 days to object and, if Cadence objects, identify an alternative sub-processor. Cadence agrees to make any objections in good faith. Vendor may provide notice by posting a list on a website that is communicated to Cadence in writing, by sending a written list to Cadence, or as otherwise agreed to in writing by the Parties.
3. **Clause 11**: the optional language will not apply.
4. **Clause 17**: Option 1 applies and the SCCs will be governed by Irish law.
5. **Clause 18(b):** Disputes shall be resolved in the courts of Ireland.

C. DATA EXPORTER & IMPORTER

Pursuant to Annex I, Part A, the Parties have identified the Data Exporter and Data Importer as described below:

Data Exporter	Cadence
Contact Details	Privacy Team, privacy@cadence.com
Company Role	Controller
Signature and Date	By entering into this DPA, Data Exporter is deemed to have signed the SCCs incorporated herein, including their Annexes, as of the Effective Date.
Description of the activities relevant to the data transferred by Data Exporter	Cadence is procuring Services from Vendor, the data importer, and in the course of receiving the Services, Cadence will need to share Cadence Data.

Data Importer	Vendor
Contact Details	As specified in the Commercial Agreement.
Company Role	Processor
Signature and Date	By entering into this DPA, Data Importer is deemed to have signed the SCCs incorporated herein, including their Annexes, as of the Effective Date.
Description of the activities relevant to the data processed by Data Importer	Vendor is processing Cadence Data Personal Data so as to perform contractual obligations as a provider of Services to Cadence.

D. DESCRIPTION OF TRANSFER

Pursuant to Annex I, Part B, the Parties agree that the data transfers are consistent with the descriptions noted below:

1. **Categories of data subjects whose personal data may be transferred:**
   - As described in Section 3.3 of the DPA.
2. **Categories of personal data transferred:**
   - As described in Section 3.4 of the DPA.
3. **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**
   - None, except where required by law to provide the Services.
4. **The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis).**
   - The frequency will be on an as-needed basis to support the work under the Commercial Agreement.
5. **Nature of the processing**
   - As described in Section 3.1 of the DPA.
6. **Purpose(s) of the data transfer and further processing**
   - As described in Section 3.2 of the DPA.
7. **The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**
   - Personal data shall be retained only so long as required to perform the Services under the Commercial Agreement.
8. **For transfers to (sub) processors, the subject matter, nature, and duration of the processing shall be as described below:**
   - Any transfers to sub-processors will be consistent with the terms of the SCCs, the Commercial Agreement, and this DPA.

E. COMPETENT SUPERVISORY AUTHORITY

For the purposes of Annex I, Part C of the SCCs, the country in which the Data Exporter is established, if applicable, shall determine the competent supervisory authority.

F. SECURITY OF PROCESSING

For the purposes of Annex II of the SCCs, Addendum C describes the required Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data.

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) and the applicable laws and regulations of the various states and territories in Australia, 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 and the California Privacy Rights Act (collectively, the "CCPA"), as amended, 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," "Third Party," and/or "Contractor".

   Vendor will process, retain, use, and disclose personal data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Cadence shall inform Vendor of any Consumer request made pursuant to the CCPA. Vendor shall delete Consumer Personal Information upon request from a Consumer and/or Cadence and shall also notify its own Service Providers, Contractors, and Third Parties to delete the Consumer's Personal Information.

   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 Consumer's Personal Data for any commercial purpose (as defined by the CCPA) other than providing the Services, (c) retain, use, or disclose Consumer's Personal Information outside of the scope of the Commercial Agreement, or (d) combine the Consumer's Personal Information with any personal information received from or on behalf of another person or persons or that it collects from its own interaction with the Consumer.

   Vendor grants Cadence the right, upon notice, to (a) take reasonable and appropriate steps to stop and remediate any unauthorized use of Consumer Personal Information and (b) monitor Vendor's compliance with this Agreement through measures, including but not limited to ongoing manual reviews and automated scans and regular assessments, audits or other technical and operational testing at least once every twelve (12) months.

   If Vendor is a Third Party, as defined by the CCPA, then Vendor shall check for and comply with a Consumer's opt-out preference signal, unless Vendor has been otherwise informed by Cadence that the Consumer has consented to the sale or sharing of their Personal Information.

   Vendor certifies that its Sub-Processors are Service Providers, Third Parties, and/or Contractors and that it shall ensure that it has a contract with such parties that contain the same requirements specified in this Agreement and Section 3 of this Addendum, as applicable. Vendor shall notify Cadence within five (5) business days of making any determination that Vendor is not able to meet its obligations under the CCPA.

4. **Canada.** "Data Protection Legislation" includes the Federal Personal Information Protection and Electronic Documents Act and any other applicable federal, provincial or territorial privacy laws and regulations, 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 and the Personal Information Protection Law.

6. **Israel.** "Data Protection Legislation" includes the Protection of Privacy Law, 5741-1981, Privacy Protection Regulations, 5761, 2001, and Protection of Privacy Regulations, 5777-2017, 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 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.

17. **United Kingdom.** "Data Protection Legislation" includes the UK Data Protection Act 2018, the UK GDPR, and other applicable UK privacy legislation, as amended.

    In the event that Cadence Data is transferred from the United Kingdom to outside the United Kingdom, 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, then the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses found at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf and issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 (the "**UK SCCs**"), shall also apply and shall prevail in case there is any conflict with the DPA and/or the Commercial Agreement.

    The UK SCCs are construed as follows:

    a. Table 1 (Part 1) shall incorporate and include the "Data Exporter" and "Data Importer" details found in the two tables in Addendum A, Section C of this DPA.

    b. Table 2 (Part 1) shall incorporate the specifications listed in Addendum A, Sections A and B, as applicable.

    c. Tables 3 and 4 shall consist of and incorporate the details specified in various sections of Addendum A and the measures described in Addendum C of this DPA, as applicable.

cadence®

ADDENDUM C: TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Vendor agrees to maintain the following minimum technical and organisational measures (for clarity, the Commercial Agreement may require heightened measures, in which case such heightened measures shall also apply):

A. Access Control to Processing Areas and Systems. Vendor shall 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;
- Individual authentication credentials such as user ID and passwords;
- 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.

B. Transmission Control. Vendor shall prevent unauthorized persons from gaining access to the personal data. 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.

C. Accountability. Vendor shall protect the data and monitor its system administrators. This includes:

- Adoption of suitable measures to register system administrators' access logs and keep them secure and accurate. destruction or loss. This includes:
    - Protecting data from accidental destruction or loss;
    - Identifying any person that carries out a data recovery procedure;
    - Recording any detected security incident; and
    - Monitoring system administrators and to ensure that they act in accordance with instructions received.