Privacy Statement

Cambridge Consultants Ltd company registration number 1036298 together with its subsidiaries Cambridge Consultants Inc. of 745 Atlantic Avenue, Boston, MA 02111, USA and Synapse Product Development Inc. of 1511 6th Ave. Ste 400, Seattle, WA 98101 asserts that the group of companies ("The Company") handles personal information in compliance with the applicable law. In the UK the Company is registered in accordance with the Data protection Act 2010 reference Z9851030. In the US the Company is registered with the Privacy Shield program, and to view the Company's certification, please visit https://www.privacyshield.gov/.

The Company is a leading, worldwide product development service provider which specializes in design engineering services, professional technical services and product technical support services ("Services"). Since the Company provides Services to clients throughout the world, onward transfer of personal data from Europe to the United States may occur. In addition, the Company may share personal data with third party agents, consultants, and contractors necessary to implement the Services. Lastly, the Company has affiliate offices throughout the world and may make use of personal data collected by other group companies.

In its role as service provider, the Company processes personal data (defined as (i) contact information including, but not limited to, a contact person's name, email address, mailing address, telephone number, title, organization name, IP address, (ii) payment information, including, but not limited to, credit card and/or bank account information and (iii) project specific information necessary to perform the Services, which may include access to sensitive personal data and (iv) personal and sensitive personal data relating to an individual's health or medical information, financial information, educational information, national identification, family or social circumstances and criminal records), for its own internal business purposes, including, without limitation, the following:

1. Maintaining and supporting its Services, delivering and providing the requested Services, and complying with its contractual obligations related thereto (including managing transactions, reporting, invoices, renewals, and other operations related to providing Services to clients and necessary third party vendors);
2. Satisfying governmental reporting, tax and other requirements;
3. Storing and processing personal data in computer databases and servers located in the United Kingdom and the United States;
4. Verifying identity for access to accounts;
5. As requested by the client and/or necessary third party agent, consultant, and contractor; and
6. As otherwise required by law.

All personal data exchanged with Company is exchanged under strict obligation of confidentiality. In addition, the exchange of personal data with Company is further restricted by limiting access to those Company personnel who need to know the personal data in order to perform the Services. All Company personnel are under individual written confidentiality agreement to only use the personal data for the purpose of the Services as directed by the Company.

In addition, the Company processes sensitive personal data as part of its human resources function for the intercompany transfer of employment for personnel in affiliate offices. The Company commits to cooperate with European Union ("EU") data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the EU in the context of the employment relationship.

No sensitive personal data is transferred to Company or any third party agent, consultant, and contractor without the informed and prior written consent of the originating data subject.

No personal information of the originating data subject is shared with: (i) a third party or (ii) for any purpose other than as originally authorized in writing by the originating data subject, without obtaining the originating data subject's prior written consent for such use. The Company provides the originating data subject the opportunity to not share its personal information or withdraw its consent at any time. The Company exchanges personal data with a third party only if: (i) the involvement of the third party agent, consultant, and contractor is necessary, (ii) the third party agent, consultant, and contractor is under confidentiality agreement to keep the personal data confidential, not share the personal data with any other party, and only use the personal data for the intended purpose for which it was originally provided, and if used for any other purpose to inform the Company and obtain Company's prior written consent before using for any other purpose) (iii) establish reasonable safeguards to ensure the third party agent, consultant, and contractor adheres to applicable privacy principles as required by law, and if such third party agent, consultant, and contractor cannot reasonably do so, refuse and/or stop the processing of any personal data to such third party. Company may be required to disclose personal data in response to a lawful request by public authorities. Company remains liable for appropriate onward transfers of personal data to third parties.

Each data subject may request a copy of their personal information from the Company by contacting the Company at data.controller@cambridgeconsultants.com. In addition, the data subject may update, amend or delete their personal data with the Company so that it is truthful, complete and accurate, in accordance with the applicable privacy laws and as further permitted by Company policy. The Company may charge a reasonable fee for access to personal data where, for example, the request for access is manifestly excessive or repetitive. Company may deny access to personal data where the burden or expense of providing access is disproportionate to the risks of the originating data subject's privacy or where right of persons other than the originating data subject would be violated. Personal data is retained only for as long as is necessary to accomplish the originally intended purpose for use of such personal data, or for as long as may be permitted or required by applicable law.

The Company commits to resolve complaints about privacy and its collection and/or use of personal data expeditiously. The Company shall respond to all privacy complaints within forty five (45) days of receipt.

The Company uses reasonable precautions to maintain the accuracy and integrity of personal data and to update it as appropriate. The Company has implemented physical and technical safeguards to protect personal data, including, for example, network access controls, passwords and access logging. The Company also protects personal data through the use of firewalls, role-based restrictions and, where appropriate, encryption technology. The Company also employs access restrictions to its physical offices.

In compliance with the Privacy Shield Principles, the Company commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding this Private Shield policy should contact the Company at data.controller@cambridgeconsultants.com. Company has further committed to refer unresolved privacy complaints to either the Information Commissioner in the UK or, , to an independent dispute resolution mechanism operated by the American Arbitration Association, International Centre for Dispute Resolution (ICDR®/AAA) based in the United States. More information about ICDR®/AAA® and its dispute resolution process may be accessed at http://info.adr.org/safeharbor. If you do not receive timely acknowledgment of your complaint from the Company or if the Company has not addressed your complaint to your satisfaction, please visit further visit the ICDR®/AAA®'s website which can be located at https://www.icdr.org/, or contact its representative Jason Cabrera by phone at +1.212.484.3207 or by email at CabreraJ@adr.org for more information or to file a complaint. The services of ICDR®/AAA® are provided at no cost to you. Finally, as a last resort and in limited situations, EU originating data subjects may seek redress from the Privacy Shield Panel, a binding arbitration mechanism. In addition, any investigation into Company's use of personal data is subject to the investigatory and enforcement powers of the Federal Trade Commission and any other U.S. authorized statutory body.

The Company has designated its internal Business Office/Legal Department to oversee compliance with applicable privacy laws. The Company will maintain, monitor, test, and upgrade information security

policies, practices, and systems to assist in protecting the personal data that it collects. Company personnel will receive training, as applicable, to effectively implement this Policy. The Company will renew its privacy certifications annually. Prior to the re-certification, the Company will conduct an in-house verification to ensure that its attestations and assertions with regard to its treatment of personal data are accurate and that the Company has appropriately implemented these practices.

This Policy may be amended from time to time, consistent with applicable data protection and privacy laws and principles. If the Company decides to materially change this Policy, the Company will post the revised Policy at this location. This Policy is not intended to, and does not create any contractual or other legal rights.

Effective June 9, 2017