Data Processing Addendum

This Data Processing Addendum (the "**DPA**") is intended to supplement the Standard Terms and Conditions of Purchase (Global) ("**Agreement**") between (i) Diodes Incorporated and its subsidiaries (collectively "**Diodes"**), and (ii) the other legal entity identified in the Agreement ("**Seller**"). For purposes of this DPA, Diodes and Seller may be referred to individually as a "**party**" and collectively as the "**parties**." In the event of a conflict between this DPA and the Agreement, the terms and conditions set forth in this DPA shall supersede and control with respect to such conflict. Any capitalized term that is used, but not otherwise defined, herein shall be ascribed the meaning set forth in the Agreement. This DPA reflects each party's understanding regarding the Processing of Personal Data by Seller for, or on the behalf of, Diodes. This DPA replaces and supersedes any previously agreed upon terms and conditions with respect to the Processing of Personal Data.

1. Definitions. For purposes of this DPA, the following terms shall apply:

California Consumer Privacy Act (CCPA)	means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and all other applicable amendments and regulations issued thereto and thereunder.
Data Protection Law	means applicable statutes, regulations, or other laws pertaining to privacy or data protection, processing of Personal Data, and/or information security, including, but not limited to, the CCPA, GDPR, UK Data Protection Law, and any other applicable international, federal, provincial, or state laws or regulations regarding information privacy that are in effect or will come into effect during the term of the Agreement.
Data Subject	means the natural person whose Personal Data is Processed by Seller under this DPA.
Documented Instructions	means the Processing terms and conditions set forth in the Agreement and this DPA.
EU Standard Contractual Clauses	means the standard contractual clauses adopted by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
General Data Protection Regulation (GDPR)	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
Information System	means any information or telecommunication system, network, equipment, hardware, or software owned or licensed by Seller to Process Personal Data.
Personal Data	means any information or data that can be used to reasonably identify a natural person, household, or device, and is subject to, or otherwise afforded protection under, an applicable Data Protection Law.
Process, Processes, Processing	means any action performed on Personal Data, including collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, transfer or otherwise making available, alignment or combination, restriction, deletion, or destruction.
Security Event	means a reasonably suspected or actual breach of security that could reasonably have led to or did lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
Sell or Sale	shall be ascribed the meaning set forth in the CCPA.
Sensitive Personal Data	means any Personal Data that is afforded special protection under a law or regulation because it could potentially cause harm, damage, or discrimination to an individual if it is disclosed, accessed, or used without authorization, and includes, but is not limited to, social security numbers and other government identifiers.
Products	means the goods and services that Seller furnishes to Diodes and/or Diodes' customers pursuant to the Agreement.
Share or Sharing	shall be ascribed the meaning set forth in the CCPA.
Subprocessor	means any third party engaged by Seller to Process Personal Data on its behalf.
United Kingdom (UK) Data Protection Law	means the GDPR as it forms part of UK law by virtue of section 3 of the UK European Union (Withdrawal) Act 2018 and the UK Data Protection Act 2018.
Chinese Personal Data Protection Law	means the applicable statutes, regulations or other laws pertaining to Personal Data protection, including, but not limited to the Personal Information Protection Law of the People's Republic of China, Security Assessment Measures for Outbound Data Transfers, Measures on the Standard Contract for Outbound Transfer of Personal Information and Implementing Rules for the Certification of Personal Information Protection.

Data Processing Addendum

2. Processing Rights and Obligations.

2.1. Roles and Responsibilities. The nature and scope of Processing Personal Data by Seller for, or the behalf of Diodes, is set forth in Annex I. For purposes of this DPA, Diodes shall be considered a "data controller" (or a "business" within the meaning of the CCPA), and Seller shall be considered a "data processor" (or a "service provider" within the meaning of the CCPA). Seller shall process Personal Data only in accordance with the Documented Instructions, except to the extent otherwise required by law. In the event Seller is compelled by law to Process Personal Data other than in accordance with the terms and conditions set forth in the Documented Instructions, Seller shall notify Diodes of that legal requirement prior to Processing, unless such notification is expressly prohibited by law.

2.2. Data Ownership. As between Diodes and Seller, Diodes retains all rights, title, and interest in the Personal Data. Diodes hereby grants to Seller a limited, revocable, nonexclusive right and license to Process the Personal Data to the extent reasonably necessary to provide, monitor, and modify the Services or as otherwise set forth herein.

2.3. CCPA Disclaimer. Each party acknowledges and agrees that the disclosure of Personal Data to the other does not constitute, and is not the intent of either party for such disclosure to constitute, a Sale or Sharing of Personal Data, and if valuable consideration, monetary or otherwise, is being provided by either party, such valuable consideration, monetary or otherwise, is being provided for the rendering of Services and not for the disclosure of Personal Data. Seller (i) shall not collect, retain, use, or disclose Personal Data for any purpose (including for any commercial purpose) other than for the specific purpose of performing the Services, unless otherwise required by law, (ii) shall not Sell or Share Personal Data, except as necessary to satisfy its obligations under the Agreement, (iii) shall not collect, retain, use, or disclose Personal Data outside the direct business relationship between Seller and Diodes, unless expressly permitted by law, and (iv) shall, at Diode's reasonable request, cease any unauthorized Processing of Personal Data and grant Diodes authorization to assess and remediate any such unauthorized Processing. This DPA is Seller's certification, to the extent the CCPA or any other applicable Data Protection Law requires such a certification, that Seller understands and will comply with the Processing limitations with respect to Personal Data that are set forth in the Documented Instructions. The parties acknowledge and agree that the "business purpose" (as the term is so used in the CCPA) for which Seller Processes Personal Data is to provide Products as described in the Agreement.

3. Diodes Obligations. Diodes shall be responsible for complying with all requirements that apply to it under applicable Data Protection Law and the Documented Instructions. Seller shall not be responsible for the accuracy, quality, or legality of Personal Data provided to Seller by Diodes. Diodes hereby represents to Seller that Diodes has the legal authority and appropriate business purpose to provide Seller with any and all Personal Data in conjunction with the Services, and when legally required, Diodes has obtained the consent from all applicable Data Subjects concerning the collection, use, disclosure, and Processing of Personal Data, as set forth herein.

4. Information Security. Seller shall (i) maintain the confidentiality of all Personal Data, (ii) implement, maintain, and continuously control and update appropriate measures designed to limit access to Personal Data to only those individuals who have a business need for such access, and (iii) take reasonable steps to ensure the reliability of all individuals who have access to Personal Data. Seller shall implement, maintain, and continuously control and update technical and organizational security controls to protect and safeguard Personal Data from a Security Event, which shall include written policies describing its security controls and measures and the relevant procedures and responsibilities of Seller personnel who have access to Personal Data ("**Information Security Program**"). Seller shall designate a senior employee to be responsible for the overall management of Seller's Information Security Program. Seller shall, upon request, respond to questionnaires and other similar requests for information regarding Seller's compliance with its Information Security Program. Without limiting the generality of the foregoing, Seller's Information Security Program shall satisfy the standards and criteria set forth in this DPA, including Annex II. If information security and cybersecurity trainings are made available by or on behalf of Diodes to Seller, Seller shall, and shall cause Seller's Personnel having access to Diodes Systems, to complete such trainings upon request by Diodes.

5. Cooperation and Assistance. Seller shall provide reasonable assistance to Diodes to enable Diodes to comply with its obligations and responsibilities under any applicable Data Protection Law, including with respect to providing access to, correcting, and deleting Personal Data in response to Data Subjects exercising their rights and privileges under applicable Data Protection Laws. Seller shall, to the extent legally permitted, promptly notify Diodes if Seller receives a correspondence, inquiry, complaint, request, or demand (collectively or individually, a "**Data Notice**") concerning the Processing of Personal Data. Notwithstanding the foregoing, in response to any such Data Notice, Seller may furnish Diodes' email contact information and request the Data Notice be submitted directly to Diodes.

Data Processing Addendum

6. Audits, Attestations, and Certifications.

6.1. Request for Information. Seller shall upon request respond to questionnaires and similar requests for information provided by Diodes to demonstrate Seller's compliance with Seller's obligations under this DPA.

6.2. Third-Party Attestations. Seller shall use independent external auditors to verify the adequacy of its written Information Security Program. Seller shall, at least annually, provide Diodes with its most recent third-party attestations, certifications, and reports relevant to the establishment, implementation, and effectiveness of Seller's Information Security Program. Diodes hereby acknowledges and agrees that any and all third-party attestations, certifications, and reports related to Seller's Information Security Program shall be deemed Seller's confidential and proprietary information.

6.3. Audits. If the information and reports described in Sections 6.1 and 6.2 of this DPA do not demonstrate, in Diodes' reasonable judgment, Seller's compliance with its obligations and responsibilities set forth in this DPA, Diodes may conduct an inspection, test (including a penetration test), or audit of Seller's business operations, or have the same conducted by a qualified third party subject to a nondisclosure agreement, provided (i) Diodes furnishes Seller advanced written notice, (ii) the inspection, test, or audit is conducted during Seller's regular business hours, and (iii) the inspection, test, or audit is conducted in a manner that does not materially interrupt Seller's business operations. Diodes shall be solely responsible for all reasonable costs and fees associated with the inspection, test, or audit described herein, unless the results demonstrate Seller's non-compliance with this DPA. Diodes shall provide the results or conclusions of any inspection, test, or audit conducted to Seller, and, unless otherwise agreed to in writing, Seller shall have thirty (30) business days from receipt of the results or conclusion to remediate or resolve any significant or material vulnerability or deficiency identified therein.

7. Return or Destruction of Personal Data. Upon termination of the Agreement, Seller shall delete or return all Personal Data in accordance with applicable Data Protection Law and certify to Diodes in writing that it has done so, provided Seller shall not be required to delete or return to Diodes any Personal Data that Seller is required by applicable law or order of a governmental or regulatory body to retain, or is required for Seller to enforce or defend its legal rights or interests under this DPA, in which case Seller shall promptly inform Diodes accordingly, including about the legal grounds for, and the term of, any further storage. Notwithstanding the foregoing, Seller shall not be required to delete or return to Diodes any Personal Data archived on backup systems if Seller securely isolates such Personal Data and protects it from any further Processing and such Personal Data is deleted in accordance with Seller's standard overwriting and deletion policies.

8 Security Event Procedures.

8.1. Response Plans. Seller shall implement and maintain its written incident response plan ("**IRP**") to identify, remediate, respond to, and recover from, a Security Event at Seller's own expense. The IRP shall include: (i) the designation of a senior employee who shall be responsible for establishing, implementing, and maintaining the IRP, (ii) the identification of internal and external resources to assist in addressing a Security Event, (iii) automated technical means to assist in the identification of activity indicative of a Security Event, (iv) processes and programs to contain and remediate the impact of a Security Event and to recover to a normal state of business operations, and (v) processes to convene a post-Security Event review to assess the effectiveness and efficiency of identifying, remediating, responding to, and recovering from, a Security Event.

8.2. Notice. Seller shall provide immediate written notice to Diodes of any Security Event after becoming aware of, or otherwise discovering, the Security Event, and this written notification shall, to the greatest extent possible, include a description of (i) the nature of the Security Event, (ii) the categories of Personal Data affected by the Security Event, (iii) the approximate number of individuals affected by the Security Event, (iv) any potential legal or regulatory consequences that may arise from the Security Event, and (v) the measures taken or proposed to be taken to address the Security Event. In the event of a Security Event, Seller shall designate a senior employee to serve as Seller's single point of contact from whom Diodes can obtain more information about the Security Event.

8.3. Assistance. Seller shall provide reasonable assistance to Diodes to (i) investigate or otherwise respond to a Security Event, and (ii) enable Diodes to meet any legal obligation it may have to give notice of the Security Event to any affected Data Subject, a governmental or regulatory authority, or any other individual or entity. Notwithstanding any other provision in the Agreement, Seller shall defend, indemnify, and hold harmless Diodes and its subsidiaries and affiliates, and each of their respective officers, directors, employees, and agents, from and against any and all claims, suits, causes of action, liability, loss, costs, and damages, including reasonable attorneys' fees, arising from or relating to a Security Event.

9. International Data Transfers.

9.1. EU Standard Contractual Clauses. To the extent any Personal Data is subject to, or otherwise afforded protection under the GDPR or UK Data Protection Law (collectively, "**EU/UK Data Protection Law**"), the parties undertake to apply the provisions of the EU Standard Contractual Clauses to the transfer and Processing of such Personal Data. If the EU Standard Contractual Clauses are applicable between the parties pursuant to this Section 9, their provisions will be deemed incorporated by reference into this DPA. To the extent required by law, the parties shall enter into and execute the EU Standard Contractual Clauses as a separate document. If the parties apply and incorporate the EU Standard Contractual Clauses pursuant to this Section 9 of this DPA, then the following shall apply: (i) the EU Standard Contractual Clauses shall be governed by the Module Two clauses (Transfer controller to processor) in all applicable instances, and Diodes shall be the data exporter and Seller shall be the data importer, (ii) each party acknowledges and agrees that Clause 7 (Optional – Docking Clause) of the EU Standard Contractual Clauses shall be deemed incorporated therein and applicable to the parties and third parties, (iii) for purposes of Clause 9(a) (Use of sub-processors) of the EU Standard Contractual Clauses, the parties agree that Option 1 (Specific Prior Authorization) shall apply to the parties, and shall be enforced in accordance with Section 7 and Annex III of this DPA, (iv) for purposes of Clause 11 (Redress) of the EU Standard Contractual Clauses, the parties agree that the optional wording shall be incorporated therein and therefore shall be applicable to the parties, (v) for purposes of Clause 17 (Governing law) of the EU Standard Contractual Clauses, the parties agree that the EU Standard Contractual Clauses shall be governed by the law of Germany and select Clause 17, "Option 2" to this effect, (vi) for purposes of Clause 18 (Choice of forum and jurisdiction) of the EU Standard Contractual Clauses, the parties agree that any dispute arising from the EU Standard Contractual Clauses shall be resolved by the Courts of Germany, (vii) Annex I of the EU Standard Contractual Clauses shall be deemed completed with the information set forth in Annex I to this DPA, (viii) Annex II of the EU Standard Contractual Clauses shall be deemed completed with the information set forth in Annex II to this DPA, and (ix) Annex III of the EU Standard Contractual Clauses shall be deemed completed with the information set forth in Annex III to this DPA and replacement Subprocessors shall be agreed upon in accordance with Section 9 of this DPA.

9.2. EU: Onward Transfers. Seller shall not transfer Personal Data received under the EU Standard Contractual Clauses (nor permit such Personal Data to be transferred) to a Subprocessor outside the EEA, unless (i) the Subprocessor is established in a country which the European Commission has granted an adequacy status, or (ii) Seller has obtained Diodes' prior written consent with respect to such transfer and Seller implements and maintains such measures as necessary to ensure the transfer is in compliance with Data Protection Law, and such measures may include (without limitation) the Subprocessor's obtaining Binding Corporate Rules authorization in accordance with Data Protection Law, or the execution by a Subprocessor and Seller of the EU Standard Contractual Clauses, Module 3 (processor to processor).

9.3. Data Transfers: Switzerland. To the extent Personal Data originates in Switzerland, the parties undertake to apply the provisions of the EU Standard Contractual Clauses, as set forth in Section 9 of this DPA (and as amended by this Section 9.3), to the transfer and Processing of such Personal Data. If the EU Standard Contractual Clauses are applicable between the parties pursuant to this Section 9.3, their provisions will be deemed incorporated by reference into this DPA, and shall apply subject to the following: (i) references to the GDPR in the EU Standard Contractual Clauses are to be understood as references to the Swiss FADP insofar as the data transfers are subject exclusively to the Swiss FADP and not the GDPR, (ii) the term "member state" in the EU Standard Contractual Clauses shall not be interpreted in such a manner as to exclude Data Subjects in Switzerland from enforcing their rights in Switzerland in accordance with Clause 18(c) of the EU Standard Contractual Clauses, provided Switzerland is their habitual residence, and (iii) for purposes of Annex I(C) of the EU Standard Contractual Clauses, (a) where the data transfer is subject exclusively to the Swiss FADP (and not the GDPR), the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and (b) where the transfer is subject to both the Swiss FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the Swiss FADP, and the supervisory authority set forth in Annex I of this DPA insofar as the transfer is governed by the GDPR.

9.4. Other Transfers. To the extent Personal Data originates outside of the EEA, Switzerland, or the UK, and the parties seek to transfer and Process such Personal Data across national borders, the parties shall also undertake to apply, as appropriate, the provisions of the EU/UK Data Protection Law to such transfer and Processing, provided that the EU Standard Contractual Clauses are legally required and sufficient to meet the requirements of the applicable Data Protection Law for the transfer and Processing of Personal Data across national borders. To the extent the parties transfer or receive Personal Data that includes Personal Data associated with identifiable individuals in mainland China, each party agrees to the terms in Annex IV.

9.5. Surveillance Disclaimers. If the parties apply and incorporate the EU Standard Contractual Clauses pursuant to Section 9 of this DPA, then Seller hereby represents and warrants the following to be true, accurate, and complete: (i) Seller

is not classified as an "electronic communication provider" or otherwise directly subject to 50 U.S.C. § 1881a ("**FISA § 702**"), (ii) has never cooperated with public authorities conducting surveillance of communications pursuant to Executive Order (EO) 12333, as amended, (iii) Seller has never been the subject of a FISA § 702 warrant, and (iv) Seller has established internal procedures and processes for responding to FISA § 702 warrants and for cooperating with national security agencies under EO 12333.

10. **Subprocessors.** Diodes hereby acknowledges and agrees that Seller may use Subprocessors to assist with its provision of Services to Diodes, provided Seller executes with any such Subprocessor a written agreement that contains terms and conditions that are substantially similar to the terms and conditions set forth in this DPA. Seller shall undertake all reasonable efforts to ensure that any such Subprocessor can comply, and is in compliance, with the terms and conditions set forth in this DPA.

11. **Indemnification.** Seller will indemnify and hold harmless Diodes and its affiliates and subsidiaries, and each of its and their officers, directors, employees, and contractors from all liabilities, suits, investigations, settlements, fines, damages, and fees (including reasonable attorneys' fees) arising out of, or in connection with, any claims, demands, investigations, or actions brought by Data Subjects or regulatory or other government authorities relating to the Personal Data Processed by Seller or any Subprocessor under, and in accordance with, this DPA.

12. **Miscellaneous.** This DPA is hereby incorporated into, and forms an integral part of, the Agreement. Each party's acceptance of the Agreement shall be deemed execution of, and agreement to, this DPA. Diodes reserves the right to periodically modify this DPA upon written notice to Seller, and such modifications will automatically become effective upon such notice from Diodes to Seller, provided such modifications are intended or otherwise designed to, in Diodes' reasonable judgment, align the activities described herein with new or amended Data Protection Laws. This DPA will be governed by and construed in accordance with governing law provisions set forth in the Agreement. References in this DPA to "writing" or "written" include e-mail communications and certified mail.

* * * * * * * * * * * * * * * * * *

Data Processing Addendum

Annex I
Data Processing Activities

A. List of parties:

Name (Data Exporter)	Diodes Incorporated or its subsidiary as set forth in the Agreement
Address	As specified in the Agreement.
Contact person's name, position and contact details	As specified in the Agreement.
Activities relevant to the data transferred under these Clauses	Set forth below (Section B, Description of Transfer).
Signature and date	By executing this DPA.
Role (controller / processor)	A data controller.

Name (Data Importer)	Seller (as set forth in the Agreement)
Address	As specified in the Agreement.
Contact person's name, position and contact details	As specified in the Agreement.
Activities relevant to the data transferred under these Clauses	Set forth below (Section B, Description of Transfer).
Signature and date	By executing this DPA.
Role (controller / processor)	A data processor.

B. Description of Transfer: Unless otherwise set forth in a statement of work, order form, or similar documentation, the description of the Personal Data transferred is as follows:

(i) Categories of Data Subjects: Diodes employees, Diodes' clients, and other third parties who receive Products via Seller, or as otherwise agreed upon in writing by the Parties.

(ii) Categories of Personal Data transferred: Employee data, HR data, client data, or as otherwise agreed upon in writing by the Parties.

(iii) Sensitive data transferred: None.

(iv) The frequency of transfer: Continuous and for so long as Diodes receives Products from Seller, and for the period thereafter, as set forth in the Agreement, or as otherwise agreed upon in writing by the Parties.

(v) Nature of Processing: To provide Products, or as otherwise agreed upon in writing by the Parties, and the Processing may include the following actions with respect to Personal Data: collection, recording, organization, storage, retrieval, use, disclosure, transfer, deletion, or destruction.

(vi) Purpose of the data transfer and further processing: Seller provides Products, and will Process Personal Data to provide these Products, to Diodes or Diodes' clients, or as otherwise agreed upon in writing by the Parties.

(vii) The period for which Personal Data will be retained: For the duration of the receipt of Products and for the time period in which Seller deletes or returns such Personal Data, as provided for in this DPA, or as otherwise agreed upon in writing by the Parties.

(viii) Subprocessor transfers: The relevant information as set forth in this DPA.

C. Competent Supervisory Authority: The competent supervisory authority in accordance with Clause 13 of the EU Standard Contractual Clauses is the supervisory authority of Germany.

Data Processing Addendum

Annex II
Security Controls

Seller's Information Security Program shall meet or exceed the information security requirements, standards, and criteria set forth in this Annex II:

1. **Asset Management**. Seller shall maintain an inventory of all media on which Personal Data is retained or transmitted and shall classify Personal Data within its custody and control. Seller shall implement and maintain policies and procedures governing the conditions and circumstances in which Seller personnel may store Personal Data on portable devices, remotely access Personal Data, and Process Personal Data outside the facilities, premises, or offices owned, leased, or operated by Seller (collectively, "**Seller Offices**").

2. **Administrative Measures; Training**. Prior to providing any of its personnel access to an Information System, Seller shall (i) ensure the reliability of such personnel, including by performing background screening (to the extent permitted by Data Protection Law), and (ii) provide appropriate security training to such personnel to ensure such personnel can comply with the obligations under this Annex II. Seller will periodically provide additional training to its personnel as may be appropriate to ensure that Seller's Information Security Program meets or exceeds prevailing industry standards.

3. **Physical Security; Business Continuity**. Seller shall establish, implement, and maintain appropriate physical security measures designed to protect Information Systems, including an access control system that enables Seller to monitor and control physical access to each Seller Office, which shall include 24x7 physical security monitoring systems and, where appropriate and reasonably necessary, the use of trained and experienced security guards. Seller shall establish, implement, and maintain a program to protect the security of its physical infrastructure from all reasonably foreseeable hazards, and a written business continuity plan to ensure the confidentiality, integrity, and availability of Personal Data during a time of emergency or disaster (a "**Business Continuity Event**"). Without limiting the generality of the foregoing, Seller shall, on an ongoing basis, but in no case less frequently than once a week, maintain back-up copies of Personal Data from which Personal Data can be recovered during a Business Continuity Event. Seller shall (i) retain back-up copies of Personal Data and data recovery procedures in a different location from where its primary Information Systems are located, (ii) implement and maintain specific procedures governing access to back-up copies of Personal Data, (iii) review data recovery procedures at least every six (6) months, and (iv) log data restoration efforts pertaining to Personal Data.

4. **Data Loss Prevention**. Seller shall implement and maintain data loss prevention processes and tools to identify, monitor and protect Personal Data in use, in transit and at rest, and such data loss prevention processes and tools shall include (i) automated tools to identify attempts of data exfiltration, (ii) the prohibition of, or secure and managed use of, portable devices, (iii) use of certificate-based security, and (iv) secure key management policies and procedures.

5. **Access Controls**. Seller shall (i) abide by the "principle of least privilege," pursuant to which Seller will permit access to Personal Data by its personnel solely on a need-to-know basis, (ii) promptly terminate its personnel's access to Personal Data when such access is no longer required for performance under the Agreement, (iii) log the details of any access to Personal Data, and retain such records for no less than ninety (90) days, and (iv) be responsible for any processing of Personal Data by its personnel.

6. **Account Management**. Seller will use reasonable measures to manage the creation, use, and deletion of all account credentials used to access an Information System, including by implementing: (i) a segregated account with unique credentials for each user, (ii) strict management of administrative accounts, (iii) password best practices, including the use of strong passwords and secure password storage, and (iv) periodic audits of accounts and credentials.

7. **System Maintenance; Segmentation**. Seller shall (i) use automated vulnerability scanning tools to continually scan Information Systems, (ii) log vulnerability scan reports, (iii) conduct periodic reviews of vulnerability scan reports over time, (iv) use patch management and software update tools for Information Systems, (v) prioritize and remediate vulnerabilities by severity, and (vi) use compensating controls if no patch or remediation is immediately available. Seller shall use reasonable measures to monitor, detect and restrict the flow of information on a multi-layered basis within Information Systems using commercially available tools and solutions, such as firewalls, proxies, and network-based intrusion detection systems.

8. **Encryption**. Seller shall encrypt, using industry standard encryption tools, Personal Data that Seller (i) transmits or sends wirelessly or across public networks or within Information Systems, (ii) stores on laptops or storage media, and (iii) stores on portable devices or within an Information System. Seller will safeguard the security and confidentiality of all encryption keys associated with encrypted information.

Data Processing Addendum

9. **Security Testing**. Seller shall, at least annually, undertake internal and external penetration, vulnerability, and application scanning and testing to assess any vulnerabilities to an Information System. Such scanning and testing shall be conducted by Seller, or (at Seller's expense) by any external qualified, credentialed, and industry-recognized auditor or consultant. Seller shall remedy vulnerabilities identified during any such scans and testing in a commercially reasonable manner and timeframe based on severity. Upon Diodes' written request, Seller will provide Diodes with any report or assessment (or summaries thereof) resulting from the scanning and testing described herein.

10. **Secure Software Development**. Seller represents and warrants that any software used in connection with the Processing of Personal Data is or has been developed using secure software development practices, including the following: (i) segregating development and production environments, (ii) filtering out potentially malicious character sequences in user inputs, (iii) using secure communication techniques, including encryption, (iv) using sound memory management practices, (v) using web application firewalls to address common web application attacks such as cross-site scripting, SQL injection and command injection, (vi) implementing the OWASP Top Ten recommendations, as applicable, (vii) patching of software, (viii) testing object code and source code for common coding errors and vulnerabilities using code analysis tools, (ix) testing of web applications for vulnerabilities using web application scanners, and (x) testing software for performance under denial of service and other resource exhaustion attacks.

Data Processing Addendum

Annex III
Approved Subprocessors

Seller will provide Diodes with a list of Subprocessors immediately upon entering into the Agreement.

Data Processing Addendum

Annex IV
Outbound Transfer of the Personal Data from Mainland China

When the parties seek to transfer Personal Data outside Mainland China, the provisions of the Chinese Data Protection Law to such transfer and processing shall apply.

1. Conditions for Transfer

When the parties need to transfer Personal Data outside Mainland China due to business or other needs, the parties shall meet any of the following conditions: (i) the parties shall pass the security assessment organized by the Cyberspace Administration of China ("**CAC**"); (ii) the parties shall have been certified by a specialized agency for protection of Personal Data in accordance with the provisions of CAC; (iii) the parties shall enter into a contract under the standard contract formulated by CAC, and apply for filing with the local cyberspace administration at the provincial level; or (iv) Other conditions stipulated by laws, administrative regulations or CAC.

1.1. Circumstance for Security Assessment. When transferring personal data outside Mainland China under any of the following circumstances, the transferring party shall apply for security assessment to CAC through the local cyberspace administration at the provincial level: (i) where the transferring party constitutes a Critical Information Infrastructure Operator ("**CIIO**"); (ii) where the transferring party processes the Personal Data of more than one million Data Subjects; or (iii) where the transferring party has provided Personal Data of one hundred thousand (100,000) Data Subjects or sensitive Personal Data of ten thousand (10,000) Data Subjects in total outside Mainland China since January 1 of the previous year.

1.2. Circumstance for Standard Contract and Certification. If the outbound data transfer does not trigger the security assessment aforesaid, the parties shall rely on Standard Contract or Certification to transfer personal data outside Mainland China.

2. Onward Transfers

The parties shall not transfer Personal Data received to a Subprocessor outside the Mainland China, unless (i) there is a genuine business necessity; (ii) the Data Subject has been fully informed about the details of the onward transfer and has given separate consent or there is another lawful basis; (iii) the Subprocessor is bound by a written agreement ensuring that the level of protection for personal data is not lower than the standards stipulated by Chinese Personal Data Protection Law, and it assumes liability for damage compensation to the Data Subject; and (iv) a copy of the written agreement with the Subprocessor will be provided to the Data Subject at his/her request.

3. Informing and Lawful Basis

The parties shall inform the Data Subject of the parties' name, contact information, processing purpose, processing method, type of Personal Data, as well as the methods and procedures for the Data Subject to exercise the rights with the parties, and obtain the Data Subject's separate consent or have other lawful basis such as (i) where it is necessary for the conclusion or performance of a contract to which the Data Subject concerned is a party, or for the implementation of human resources management in accordance with the labor rules and regulations formulated in accordance with the law and the collective contract concluded in accordance with the law; (ii) where it is necessary for the performance of statutory duties or statutory obligations; (iii) where it is necessary for the response to a public health emergency or for the protection of the life, health and property safety of a Data Subject in an emergency; (iv) where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the handling of Personal Data is within a reasonable scope; (v) where it is necessary to process the Personal Data disclosed by the Data Subject concerned or other Personal Data that has been legally disclosed within a reasonable scope in accordance with the provisions of Chinese Personal Data Protection Law; and (vi) other circumstances prescribed by Chinese laws and administrative regulations.

4. Personal Data Protection Impact Assessment Report and Record of Processing

Before transferring Personal Data outside Mainland China, the parties shall conduct a Personal Data Protection Impact Assessment ("**PDPIA**") and record the processing details. The PDPIA report and records shall be retained for at least three (3) years.

Data Processing Addendum

5. Security Measures

The parties shall, according to the purpose and method of processing Personal Data, types of Personal Data, impacts on personal rights and interests and possible security risks, take the following measures to ensure the compliance of Chinese Personal Data Protection Laws and prevent unauthorized access and divulgence, falsification and loss of Personal Data: (i) formulating internal management systems and operating procedures; (ii) implementing category-based management of Personal Data; (iii) taking corresponding technical security measures such as encryption and de-identification; (iv) reasonably determining the authority to process Personal Data and conducting security training for relevant employees on a regular basis; and (v) formulating and organizing the implementation of emergency plans for Security Event.

6. Details of outbound transfer of the Personal Data in accordance with this Agreement

6.1. Purpose of processing: Seller provides Products as listed in the Agreement and will process Personal Data to provide these Products to Diodes or Diodes' customers, or as otherwise agreed upon in writing by the parties.

6.2. Method of processing: To provide Products, or as otherwise agreed upon in writing by the parties, and the processing may include the following actions with respect to Personal Data: collection, recording, organization, storage, retrieval, use, disclosure, transfer, deletion, or destruction.

6.3. Scale of the Personal Data transferred abroad: Only as required for Seller to provide the Products as listed in the Agreement.

6.4. Types of the Personal Data transferred abroad (referenced is made to GB/T 35273 Information Security Technology—Personal Information Security Specification and related standards): Employee data, HR data, client data, or as otherwise agreed upon in writing by the parties.

6.5. Types of the Sensitive Personal Data transferred abroad (if applicable, reference is made to GB/T 35273 Information Security Technology—Personal Information Security Specification and related standards): None.

6.6. The Overseas Recipient only provides the Personal Data to the following third parties outside Mainland China (if applicable): The relevant information on subprocessing is as set forth in this DPA.

6.7. Transfer method: Electronic or physical submission of a purchase order or electronic mail, or as otherwise agreed upon in writing by the parties.

6.8. Storage period after being transferred abroad: For the duration of receipt of the Product(s) from Seller and for the time period in which Seller deletes or returns such Personal Data, as provided for in this DPA.

6.9. Storage place after being transferred abroad: Seller's Information Systems and Seller Offices, or as otherwise agreed upon in writing by the parties.

6.10. Other matters (to be filled in as appropriate):