**Data Protection Agreement for onsemi and Approved Vendors**

This is a Data Protection Agreement (this “DPA”) between Semiconductor Components Industries, LLC, a limited liability company organized under the laws of Delaware, with offices at 5701 N. Pima Road, Scottsdale. AZ 85250[[1]](#footnote-2) (“onsemi”) and Vendor Company (“Processor”) (onsemi and Processor shall be known as the “Parties”). The Parties do business pursuant to which the Processor provides services to onsemi in its capacity as, between the Parties, the “Controller” (collectively, the “Services”) that may entail the Processing of Personal Data (as defined below). The Parties may have one or more existing agreements (the “Agreements”).

As the governing laws of various jurisdictions impose specific due diligence and contractual obligations on onsemi with regard to its vendor relationships, the Parties are required to comply with all Applicable Privacy and Data Protection Laws and Regulations (as defined below), including but not limited to, the European Union’s (“EU’s”) and the United Kingdom’s General Data Protection Regulation (“GDPR”)[[2]](#footnote-3), Japan’s Act on the Protection of Personal Information (“APPI”)[[3]](#footnote-4), the Philippines Data Privacy Act of 2012 (“Philippines DPA”)[[4]](#footnote-5) and its Implementing Rules and Regulations (“Philippines DPA IRR”), the Vietnamese Protection of Personal Data Decree 13/2023/ND-CP (“Vietnamese DPDD”)[[5]](#footnote-6), the Personal Information Protection Law (“PIPL”) of the People’s Republic of China (the “PRC”) and the California Consumer Privacy Act, as amended from time to time (collectively, “CCPA”).[[6]](#footnote-7)

The Parties are required and agree to implement this DPA and the related Agreements pursuant to Applicable Privacy and Data Protection Laws and Regulations. This DPA and the related Agreements are hereby incorporated by reference into any and all Agreements in order to demonstrate the Parties’ compliance with Applicable Privacy and Data Protection Laws and Regulations. In the absence of any Agreements, this DPA shall stand alone as an Agreement between the Parties.

This DPA will remain in full force and effect so long as (i) the Agreements remain in effect; or (ii) the Processor retains any Personal Data related to this DPA in its possession or control, whichever is the longer.

1. For the purposes of this DPA, the definitions are as follows:

1. “Applicable Privacy and Data Protection Laws and Regulations” means all laws and regulations relating to the Processing of Personal Data, including but not limited to such laws and regulations of :
   * + the EU, the European Economic Area (“EEA”) and its member states and Switzerland;
     + the United Kingdom (including the Data Protection Act 2018, the GDPR, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003); and
     + the PRC, Vietnam, the Philippines and other APEC regions, and the United States, including federal as well as state laws in California and other states, applicable to the Processing of Personal Data under this DPA,

and shall include any amendment or replacement of such laws or regulations from time to time.

1. “Controller” means a natural or legal person, or organization which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
2. “Data Subject” means the identified or identifiable person to whom Personal Data relates.
3. “Personal Data “means any information relating to (i) an identified or identifiable natural person, and (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information) under Applicable Data Protection Laws and Regulations.
4. “Personal Data Breach” means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
5. “Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
6. “Processor” means the entity which Processes Personal Data on behalf of the Controller.
7. “Standard Contractual Clauses (EU/EEA)” means the Standard Contractual Clauses (MODULE TWO: Transfer controller to processor), dated 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, as described in Article 46 of the GDPR and approved by European Commission Implementing Decision (EU) 2021/91.
8. “Standard Contractual Clauses (UK)” means the Standard Contractual Clauses (Processors), dated 5 February 2010, for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR, approved by European Commission Decision 2010/87/EU and recognized by the regulatory or supervisory authorities of the United Kingdom for use in connection with data transfers from the United Kingdom.
9. “Subprocessor” means any processor hired on behalf of the Processor (including any affiliate of the Processor).
10. “Transfer” means to disclose or otherwise make Personal Data available to a third party (including to any affiliate or Subprocessor), either by physical movement of the Personal Data to a third party or by enabling access to the Personal Data by other means.

2. Processor shall at all times implement appropriate technical and organizational measures, including but not limited to the security measures set out in Annex 2, against unauthorized or unlawful Processing of Personal Data and against Personal Data Breaches in such a manner that its Processing of Personal Data will meet the requirements of Applicable Privacy and Data Protection Laws and Regulations and ensure the protection of the rights of the Data Subjects.

3. For all Personal Data:

1. Annex 1 describes the subject matter, nature and purpose of Processing and the Personal Data categories and Data Subject types in respect of which the Processor may Process to provide its Services under the Agreements. The duration of the Processing will be the same as the duration of the Agreements, except as otherwise agreed to in writing by the Parties.
2. In accordance with Applicable Privacy and Data Protection Laws and Regulations (including Article 28(2) of the GDPR and similar laws (e.g., Section 1798.140(w)(2) of the California Civil Code, Sections 23-24 of Japan’s APPI, Vietnamese DPDD and Philippines IRR law)):
   1. onsemi hereby provides general authorization to the Processor to engage Subprocessors. The Processor shall inform onsemi at least thirty (30) days before implementing any intended changes concerning the addition or replacement of Subprocessors (including the identity, location and intended processing activities to be performed by the Subprocessor) and give onsemi the opportunity to object to such changes. The Processor shall also comply with the requirements for Subprocessing as set forth in Applicable Privacy and Data Protection Laws and Regulations and, where applicable, the Standard Contractual Clauses (EU/EEA) or the Standard Contractual Clauses (UK), namely that the data protection obligations set forth herein (and as may otherwise be agreed by the Processor in the Agreements) shall be imposed upon the Subprocessor, so that the Processor is fully liable for any acts or omissions by the Subprocessor, and the Processor’s contract with the Subprocessor (i) contains sufficient guarantees that the Processing will meet the requirements of Applicable Privacy and Data Protection Laws and, where applicable, the Standard Contractual Clauses (EU/EEA) or the Standard Contractual Clauses (UK), and (ii) imposes the same obligations on the Subprocessor as are imposed on the Processor under this DPA.
   2. Any written contract between Processor and its Subprocessor shall provide for a third-party beneficiary clause for cases where the Data Subject is not able to bring a claim for compensation against the controller because it has factually disappeared or has ceased to exist in law or has become insolvent and no successor entity has assumed the entire legal obligations of the controller by contract or by operation of law. Such third-party liability of the Subprocessor shall be limited to its own processing operations under its subprocessing contract with Processor.
3. The Parties agree to the following:
4. The Processor shall only Process the Personal Data (i) as needed to provide the Services, (ii) in accordance with the specific instructions that it has received from onsemi, including with regard to any Transfers, and (iii) as needed to comply with a legal requirement (in which case, the Processor shall provide prior notice to onsemi of such legal requirement, unless that law prohibits this disclosure);
5. The Processor receiving Personal Data from onsemi is expressly prohibited from selling the Personal Data; retaining, using, or disclosing the Personal Data for any other purpose other than the specific purpose of performing the Services specified in the Agreements, including retaining, using, or disclosing the Personal Data for a commercial purpose other than providing the Services specified in the Agreements; and retaining, using, or disclosing the Personal Data outside of the direct business relationship between the Data Subject and onsemi.
6. Processor shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
7. Processor shall take all security measures required by Article 32 of the GDPR, and other Applicable Privacy and Data Protection Laws and Regulations (e.g., Vietnamese DPDD, Philippines DPA, Philippines DPA IRR, and other issuances of the National Privacy Commission (“NPC”)); namely:
8. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the security measures set out in Annex 2, and inter alia as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.
9. In assessing the appropriate level of security, account shall be taken, in particular, of the risks that are presented by Processing, in particular with respect to a Personal Data Breach.
10. The Processor shall take steps to ensure that any natural person acting under the authority of the Processor who has access to Personal Data does not Process them except on instructions from onsemi unless he or she is required to do so by Applicable Privacy and Data Protection Laws and Regulations.
11. Considering the nature of the Processing, Processor (i) shall reasonably assist onsemi by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of onsemi’s obligation to respond to requests for exercising the Data Subjects’ rights, and (ii) shall not (and shall ensure that any of its Subprocessors do not) object to a Data Subject being represented by an association or other body if the Data Subject so expressly wishes and if permitted by applicable national law;
12. Taking into account the nature of Processing and the information available to the Processor, Processor shall comply with (and shall reasonably assist onsemi to comply with) all Applicable Privacy and Data Protection Laws and Regulations (e.g.,: obligations set forth by the Vietnamese DPDD, Philippines DPA, the Philippines DPA IRR, other relevant laws, and other issuances of the NPC, and obligations under the PRC’s PIPL), the obligations regarding Personal Data Breaches (e.g., as set forth in Articles 33 and 34 of the GDPR), data protection impact assessments (as set forth in Article 35 of the GDPR), cross-border data transfers (e.g., as set forth in Article 38 of PRC’s PIPL) and prior consultation (as set forth in Article 36 of the GDPR);
13. At onsemi’s discretion and upon request, or as otherwise required under applicable law, the Processor shall delete or return all the Personal Data to onsemi after the end of the provision of Services relating to Processing, and delete existing copies unless the Applicable Privacy and Data Protection Laws and Regulations (e.g., EEA member state law) require continued storage of the Personal Data by Processor;
14. The Processor shall provide (and shall ensure that its Subprocessors provide) onsemi with all information necessary to demonstrate compliance with the obligations laid down in Applicable Privacy and Data Protection Laws and Regulations (ex: GDPR and Philippines DPA, Philippines DPA IRR, Vietnamese DPDD, or any other issuance of the NPC), and allow for and contribute to audits, including inspections, conducted by onsemi or another auditor mandated by onsemi, or a supervisory authority; and the Processor shall immediately inform onsemi if, in its opinion, an instruction infringes Applicable Privacy and Data Protection Laws and Regulations (e.g., the GDPR other Union or Member State data protection provisions, or the Vietnamese DPDD, Philippines DPA, Philippines DPA IRR, or any other issuance of the NPC). Notification of the potential infringement shall be sent to the onsemi Privacy Office (Privacy@onsemi.com) and the business unit at onsemi who primarily interacts with the Processor.
15. If and to the extent Applicable Privacy and Data Protection Laws and Regulations require the implementation of appropriate safeguards for any Transfer of Personal Data originating in the EU/EEA or the United Kingdom to the Processor (where onsemi or any of its affiliates is the entity exporting Personal Data to the Processor outside the EU/EEA and the United Kingdom), such Transfer shall be subject, as appropriate in the individual case, to the Standard Contractual Clauses (EU/EEA) or the Standard Contractual Clauses (UK), which are hereby incorporated into this DPA by reference. The Standard Contractual Clauses (EU/EEA) and the Standard Contractual Clauses (UK) shall apply as follows:
16. The “data exporter” shall be onsemi or its affiliate Transferring Personal Data from the EU/EEA or from the United Kingdom;
17. The “data importer” shall be the Processor;
18. In relation to a Transfer of Personal Data originating in the EU/EEA, the Standard Contractual Clauses (EU/EEA) shall be deemed to be completed as follows:
19. In Clause 7, the optional docking clause will apply;
20. In Clause 9(a), Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 3.B.1 of this DPA;
21. In Clause 11, the optional language will not apply;
22. In Clause 17, Option 1 will apply, and the Standard Contractual Clauses (EU/EEA) will be governed by the law of Belgium;
23. As per Clause 18(b), disputes shall be resolved before the courts of Belgium;
24. Annex I of the Standard Contractual Clauses (EU/EEA) shall be deemed completed with the information set out in Annex 1 to this DPA;
25. Annex II of the Standard Contractual Clauses (EU/EEA) shall be deemed completed with the information set out in Section 2 of this DPA and Annex 2 to this DPA.
26. In relation to a Transfer of Personal Data originating in the United Kingdom, the Standard Contractual Clauses (UK) shall be deemed to be completed as follows:
27. Appendix 1 of the Standard Contractual Clauses (UK) shall be deemed completed with the information set out in Annex 1 to this DPA;
28. Appendix 2 of the Standard Contractual Clauses (UK) shall be deemed completed with the information set out in Section 2 of this DPA and Annex 2 to this DPA.
29. In the event of a conflict between (i) this DPA or any Agreement, and (ii) the Standard Contractual Clauses (EU/EEA) or the Standard Contractual Clauses (UK), the latter shall prevail.
30. The Processor shall not Transfer any Personal Data (and shall not permit its Subprocessors to Transfer any Personal Data) to a Subprocessor without the prior consent of onsemi. The Processor understands that onsemi must first approve and document that adequate protection for the Personal Data will exist after the Transfer, using contracts that provide sufficient guarantees (such as the Standard Contractual Clauses (EU/EEA) and the Standard Contractual Clauses (UK)) or another legal basis for the Transfer in accordance with and to the extent allowed by Applicable Privacy and Data Protection Laws and Regulations. Upon receiving consent from onsemi to Transfer any Personal Data to any Subprocessor, the Processor shall only make such Transfer in compliance with (and shall ensure that its Subprocessors making any Transfer comply with) the provisions set forth or referenced in this DPA.
31. **The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will promptly notify onsemi (i.e., within 48 hours unless a shorter period is required under applicable law) without undue delay in the event of any Personal Data Breach. Notification shall be sent to the onsemi Privacy Office (**[**Privacy@onsemi.com**](mailto:Privacy@onsemi.com)**), the Cyber Incident Response Team (**[**CIRT@onsemi.com**](mailto:CIRT@onsemi.com)**), and the business unit at onsemi who primarily interacts with the Processor.**
32. The Processor shall maintain all agreements that it concludes with its Subprocessors, and records required by all Applicable Privacy and Data Protection Laws and Regulations, including Article 30(2) of the GDPR and/or the EU-U.S. Data Privacy Framework, and (to the extent they are applicable to Processor’s activities for onsemi) Processor shall make them available to onsemi upon request.
33. Processor will notify onsemi promptly if Processor: (i) has reason to believe that it is unable to comply with any of its obligations under this DPA and it cannot cure this inability to comply within a reasonable timeframe; or (ii) becomes aware of any circumstances or change in applicable law that is likely to prevent it from fulfilling its obligations under this DPA. In the event Processor provides such notice, onsemi will have the right to temporarily suspend the relevant Processing under this DPA until such time that the Processing is adjusted in such a manner that the noncompliance is remedied. To the extent such adjustment is not possible, onsemi will have the right to terminate this DPA and the Agreements, without liability to onsemi.

The Parties agree and accept this DPA as of the date of the last signed by the duly authorized representatives of the respective Parties.

|  |  |
| --- | --- |
| **SEMICONDUCTOR COMPONENTS INDUSTRIES, LLC[[7]](#footnote-8)**  Signature:  Printed Name:  Signatory Title: | **PROCESSOR**  [ADD LEGAL NAME OF PROCESSOR AND REMOVE PARENS.]  Signature:  Printed Name:  Signatory Title |
| Date: | Date: |

**Annex 1**

**List of Parties and Description of Transfer**

**A. List of Parties**

**Data exporter(s)**: onsemi or its affiliate Transferring Personal Data from the EU/EEA or from the United Kingdom.

Name: see page 1 of the DPA.

Address: see page 1 of the DPA.

Contact person’s name, position and contact details: Paul Dutton, Chief Privacy Officer, 5701 N. Pima Road, Scottsdale, AZ 85250, (602) 244-3250, [Paul.Dutton@onsemi.com](mailto:Paul.Dutton@onsemi.com); Ann Hill, Privacy Attorney, [Ann.Hill@onsemi.com](mailto:Ann.Hill@onsemi.com)

Activities relevant to the data transferred under these Clauses: The data exporter is the user of professional Services as described in the DPA or the Agreement(s).

Signature and date: see the DPA (the Standard Contractual Clauses (EU/EEA) and the Standard Contractual Clauses (UK) are incorporated into the DPA by reference).

Role (controller/processor): controller.

**Data importer(s)**: Processor (as defined on page 1 of the DPA).

Name: see page 1 of the DPA.

Address: see page 1 of the DPA.

**Contact person’s name, position and contact details: see Agreement(s) or enter below.**

Activities relevant to the data transferred under these Clauses: The data importer is the provider of the Services described in the Agreement(s).

Signature and date: see the DPA (the Standard Contractual Clauses (EU/EEA) and the Standard Contractual Clauses (UK) are incorporated into the DPA by reference).

Role (controller/processor): processor.

**B. Description of Transfer**

**Categories of data subjects whose personal data is transferred:**

The Personal Data transferred concern the following categories of data subjects:

* Employees, contractors and other staff of onsemi
* onsemi’s customers and business partners

**Purpose(s) of the data transfer and further processing**

The transfer is made for the following purposes:

* For the purposes of Processor providing the Services to onsemi under the Agreements.

**Categories of Personal Data Being Transferred**

The Personal Data transferred concern the following categories of data:

a) Categories of data relating to employees, contractors and other staff of onsemi:

* name, position, identifiers, contact details (personal or business)
* other incidental Personal Data contained in internal documents, correspondence or commercial contracts such as addresses, dates of birth, family, government or company issued numbers, and the like

b) Categories of onsemi’s customers:

* name, position, contact details (personal or business)
* other incidental Personal Data contained in correspondence or commercial contracts

**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 specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

[ ] Not applicable

***OR***

The **special categories of data transferred concern the following categories of data:**

* [insert types of special categories of data that will be processed from list in footnote]
* [insert types of restrictions or safeguards applied in accordance with the examples provided above][[8]](#footnote-9)

**Nature of the processing**

The Personal Data transferred will be subject to the following basic Processing activities - collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination and otherwise making available, alignment or combination, restriction, erasure and destruction.

**The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)**

Continuous as part of the Services provided by the data importer.

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

At the end of the Services provided by the data importer related to the Processing of Personal Data under the Agreement(s), the data importer shall delete or return the Personal Data in accordance with Section 3.C.7 of the DPA.

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**

In accordance with the DPA, the data importer may engage other companies to provide limited services that constitute a subset of the Services provided by the data importer under the Agreement(s). Any such subcontractors will be permitted to Process Personal Data only as necessary to deliver the services the data importer has retained it to provide and is prohibited from using Personal Data for any other purpose. Unless a particular subcontractor is replaced ahead of time, the Processing will be for the term designated under the applicable Agreement(s).

**C. Competent supervisory authority[[9]](#footnote-10)**

Identify the competent supervisory authority/ies in accordance with Clause 13 of the Standard Contractual Clauses (EU/EEA):

Belgian Data Protection Authority: Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)

**Annex 2**

**Security Standards**

Processor operates and maintains an information security program based on a relevant industry framework such as National Institute of Standards and Technology (NIST) Cybersecurity Framework, and enforces various policies, standards and processes designed to secure Personal Data and other data to which Processor personnel are provided access and to protect Personal Data and other data from accidental loss or destruction. The following is a description of some of the minimum core technical and organizational security measures implemented by Processor.

This Annex 2 represents the minimum security measures that will be taken by Processor.

* 1. **Information Security Policies and Standards**

Processor will implement security requirements for staff and all subcontractors, vendors or agents who have access to Personal Data that are designed to ensure a level of security appropriate to the risk and address the requirements detailed in these Security Standards. Processor will conduct periodic risk assessments and review and, as appropriate, revise its information security practices at least annually or whenever there is a material change in Processor’s business practices that may reasonably affect the security, confidentiality or integrity of Personal Data, provided that Processor will not modify its information security practices in a manner that will weaken or compromise the confidentiality, availability or integrity of Personal Data. Processor shall keep written records of such assessments and reviews. Processor will have in place documents that specify its policies and practices in relation to Personal Data that are accessible to the Data Subject, such as an online privacy policy.

* 1. **Physical Security**

The Processor will maintain commercially reasonable security systems at all Processor sites at which an information system that uses or houses Personal Data is located. The Processor reasonably and appropriately restricts access to such Personal Data and has in place practices to prevent unauthorized individuals from gaining access to Personal Data.

* 1. **Organizational Security**
* Processor will maintain records specifying which media are used to store Personal Data.
* When media are to be disposed of or reused, procedures have been implemented to prevent any subsequent retrieval of any Personal Data stored on the media before they are withdrawn from the inventory. When media are to leave the premises at which the files are located as a result of maintenance operations, procedures have been implemented to prevent undue retrieval of Personal Data stored on them.
* Processor will implement security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.
* All Personal Data security incidents are managed in accordance with appropriate incident response procedures.
  1. **Network Security**

The Processor maintains network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection and/or prevention systems, access control lists and routing protocols.

* 1. **Change Management**

The Processor will implement and maintain a change management process to properly identify, document and authorize configuration changes within the Processor’s information technology environment.

* 1. **Technical Vulnerability Management**

The Processor will implement and maintain a technical vulnerability management process that ensures information systems used by Processor are regularly monitored for technological vulnerabilities and appropriate measures taken to address the risk involved. The Processor will notify onsemi of critical and high severity vulnerabilities, as defined by NIST, that may impact the systems processing Personal Data if appropriate and timely measures cannot be taken to address the risk involved.

* 1. **Incident Response and Management**

The Processor will implement, maintain and test a comprehensive incident response and management process designed to address and manage actions required by Processor as a result of a cyber attack or network security breach.

* 1. **Access Control**
* Processor will maintain appropriate access controls, including, but not limited to, restricting access to Personal Data to the minimum number of Processor personnel who require such access.
* Privileged access is granted only to authorized individuals who have a need to know and may only to used to perform approved duties.
* Only authorized staff can grant, modify or revoke access to an information system that uses or houses Personal Data. Processor will maintain an audit log.
* User administration procedures define user roles and their privileges, and how access is granted, changed and terminated; address appropriate segregation of duties; and define the logging/monitoring requirements and mechanisms.
* All employees of the Processor are assigned unique User IDs.
* Access rights are implemented adhering to the “principle of least privilege.”
* Processor will implement commercially reasonable physical and electronic security to create and protect passwords.
  1. **Encryption**

Processor will encrypt, using secure industry-standard encryption tools, all sensitive Personal Data that Processor: (i) transmits or sends wirelessly or across public networks; (ii) stores on laptops or storage media; or (iii) stores on portable devices. Processor will safeguard the security and confidentiality of all encryption keys associated with encrypted sensitive Personal Data. onsemi further requires that the Processor will not have access to the decryption keys. onsemi exclusively would be able to decrypt Personal Data in its own environment.

* 1. **Virus and Malware Controls**

The Processor will install and maintain industry leading anti-virus and malware protection software on the system to protect Personal Data from anticipated threats or hazards and protect against unauthorized access to or use of Personal Data. All Processor Systems shall be routinely checked for computer viruses and malware, using up-to-date anti-malware software in accordance with industry recognized practices.

* 1. **Personnel**

Processor will require personnel to comply with these Security Standards prior to providing personnel with access to Personal Data.

The Processor will conduct criminal background checks, at its own expense, for staff (employees and authorized consultants) and confirm that criminal background checks have further been completed for all subcontractors, vendors or agents with access to Personal Data.

The Processor will implement a security awareness program to train personnel about their security obligations. This program includes training about data classification obligations; physical security controls; security practices; and security incident reporting.

* 1. **Business Continuity**

The Processor will implement and test appropriate disaster recovery and business continuity plans. These plans will include processes to seek recovery of Personal Data that was modified or destroyed due to unauthorized access. Processor will regularly review and update its business continuity plan to ensure it is current and effective.

* 1. **Primary Security Manager**

Processor will notify onsemi of its designated primary security manager upon request. The security manager will be responsible for managing and coordinating the performance of Processor’s obligations set forth in this DPA.

1. For purposes of this Agreement, the following entities are covered under this DPA: add entity/affiliate of onsemi and remove highlight [↑](#footnote-ref-2)
2. For purposes of this DPA, “GDPR” means Regulation (EU) 2016/679 together with any implementing or supplementing legislation, rules or regulations issued by applicable supervisory authorities. In connection with the United Kingdom, “GDPR” means Regulation (EU) 2016/679 as it forms part of the law of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018 and the UK Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019. [↑](#footnote-ref-3)
3. https://www.ppc.go.jp/files/pdf/Act\_on\_the\_Protection\_of\_Personal\_Information.pdf [↑](#footnote-ref-4)
4. https://www.privacy.gov.ph/data-privacy-act/ [↑](#footnote-ref-5)
5. https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-No-13-2023-ND-CP-dated-April-17-2023-on-protection-of-personal-data/564343/tieng-anh.aspx [↑](#footnote-ref-6)
6. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\_id=201720180SB1121 [↑](#footnote-ref-7)
7. onsemi contracting entity. [↑](#footnote-ref-8)
8. onsemi to coordinate with respect to the applicable vendor arrangement. For reference, sensitive data would include personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person’s sex life or sexual orientation. [↑](#footnote-ref-9)
9. Where the Standard Contractual Clauses (EU/EEA) do not apply and an EU/EEA data transfer is absent, this DPA shall be subject to the same choice-of-law jurisdiction as specified in the supplemental commercial agreements with the Processor. [↑](#footnote-ref-10)