**Data Protection Agreement for ON Semiconductor 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 5005 E. McDowell Rd., Phoenix, AZ 85008][[1]](#footnote-2) (“ON Semiconductor”) and Vendor Company (“Processor”) (ON Semiconductor and Processor shall be known as the “Parties”). The Parties do business pursuant to which the Processor provides services to On Semiconductor 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 ON Semiconductor 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”) 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”), and the California Consumer Privacy Act (“CCPA”).[[5]](#footnote-6)

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 as it forms part of the law of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018, 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 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. “Subprocessor” means any processor hired on behalf of the Processor (including any affiliate of the Processor).
8. “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, and Philippines IRR law)):
	1. The Processor shall not engage any Subprocessor without prior specific or general written authorization of ON Semiconductor. In the case of general written authorization, the Processor shall inform ON Semiconductor of 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 ON Semiconductor 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, 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 (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 ON Semiconductor, 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 ON Semiconductor of such legal requirement, unless that law prohibits this disclosure);
5. The Processor receiving Personal Data from ON Semiconductor 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 On Semiconductor.
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., 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 ON Semiconductor 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 ON Semiconductor by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of ON Semiconductor’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 ON Semiconductor to comply with) all Applicable Privacy and Data Protection Laws and Regulations (e.g.,: obligations set forth by the Philippines DPA, the Philippines DPA IRR, other relevant laws, and other issuances of the NPC), 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), and prior consultation (as set forth in Article 36 of the GDPR);
13. At ON Semiconductor’s discretion, the Processor shall delete or return all the Personal Data to ON Semiconductor 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) ON Semiconductor 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, or any other issuance of the NPC), and allow for and contribute to audits, including inspections, conducted by ON Semiconductor or another auditor mandated by ON Semiconductor, or a supervisory authority; and the Processor shall immediately inform ON Semiconductor 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 Philippines DPA, Philippines DPA IRR, or any other issuance of the NPC). Notification of the potential infringement shall be sent to the ON Semiconductor Privacy Office (Privacy@onsemi.com) and the business unit at ON Semiconductor who primarily interacts with the Processor.
15. If any Transfer between ON Semiconductor and the Processor requires execution of the EU Standard Contractual Clauses (Controller to Processor) (where ON Semiconductor or any of their affiliates is the entity exporting Personal Data to the Processor outside the EEA or the UK), the parties will execute such terms in Annex 3 and take all other actions required to legitimise the Transfer. If the transitional period under the UK - EU Withdrawal Agreement (OJEU L 29/7) expires before the European Commission has adopted an adequacy decision in respect of the UK then the parties will amend the terms of Annex 3 if so required to accommodate any export of Personal Data from ON Semiconductor or any of their affiliates from the EEA to the Processor in the UK.
16. 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 ON Semiconductor. The Processor understands that ON Semiconductor 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 EU Standard Contractual Clauses) 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 ON Semiconductor 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 in this DPA.
17. The Processor will promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of the Personal Data. Processor will promptly notify ON Semiconductor (i.e., within 48 hours) without undue delay in the event of any Personal Data Breach. Notification shall be sent to the ON Semiconductor Privacy Office (Privacy@onsemi.com), the Cyber Incident Response Team (CIRT@onsemi.com), and the business unit at ON Semiconductor who primarily interacts with the Processor.
18. 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 (to the extent they are applicable to Processor’s activities for ON Semiconductor) Processor shall make them available to ON Semiconductor upon request.
19. Processor will notify ON Semiconductor 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, ON Semiconductor 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, ON Semiconductor will have the right to terminate this DPA and the Agreements, without liability to ON Semiconductor.

The Parties agree and accept this DPA as of the date of the last signed by the Parties.[[6]](#footnote-7)

|  |  |
| --- | --- |
| **[SEMICONDUCTOR COMPONENTS INDUSTRIES, LLC][[7]](#footnote-8)**Signature:Date: | **PROCESSOR**Signature:Date: |
|  |  |

**Annex 1**

**Description of Transfer**

**Data subjects**

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

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

**Purposes of the transfer(s)**

The transfer is made for the following purposes:

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

**Categories of data**

The Personal Data transferred concern the following categories of data:

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

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

b) Categories of ON Semiconductor’s customers:

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

**[Special categories of data (if appropriate)**

[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]][[8]](#footnote-9)

**Processing operations**

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.

**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 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.

* 1. **Incident Response and Management**

The Processor will implement and maintain 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.
* 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.
* ON Semiconductor will establish security procedures to prevent Personal Data Processing systems from being used accidentally or without authorization, such as through logical access controls.
	1. **Encryption**

Processor will encrypt, using 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. ON Semi further requires that the Processor will not have access to the decryption keys. ON Semi 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.

* 1. **Personnel**

Processor will require personnel to comply with these Security Standards prior to providing personnel 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 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 ON Semiconductor 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.

Annex 3

STANDARD CONTRACTUAL CLAUSES

(CONTROLLER TO PROCESSOR)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, the data exporter and the data importers identified in the signature pages to these clauses, each a “party; together “the parties”, HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

1. Definitions

For the purposes of the Clauses:

* + 1. ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data([[9]](#footnote-10));
		2. ‘the data exporter’ means the controller who transfers the personal data;
		3. ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
		4. ‘the subprocessor’ means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
		5. ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
		6. ‘technical and organizational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
1. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

1. Third-party beneficiary clause
	1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
	2. The data subject can enforce against the dataimporter this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
	3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
	4. The parties 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 national law.
2. Obligations of the data exporter

The data exporter agrees and warrants:

* + 1. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
		2. that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter’s behalf and in accordance with the applicable data protection law and the Clauses;
		3. that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
		4. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
		5. that it will ensure compliance with the security measures;
		6. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
		7. to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
		8. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
		9. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
		10. that it will ensure compliance with Clause 4(a) to (i).
1. Obligations of the data importer([[10]](#footnote-11))

The data importer agrees and warrants:

* + 1. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
		2. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
		3. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;
		4. that it will promptly notify the data exporter about:
			1. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
			2. any accidental or unauthorized access, and
			3. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
		5. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
		6. at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
		7. to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
		8. that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
		9. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
		10. to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.
1. Liability
	1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
	2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

* 1. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.
1. Mediation and jurisdiction
	1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
		1. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
		2. to refer the dispute to the courts in the Member State in which the data exporter is established.
	2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.
2. Cooperation with supervisory authorities
	1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
	2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
	3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).
3. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

1. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

1. Subprocessing
	1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by wayof a written agreement with the subprocessor which imposes the same obligations on the subprocessor as areimposed on the data importer under the Clauses([[11]](#footnote-12)). Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor’s obligations under such agreement.
	2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
	3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
	4. The dataexporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter’s data protection supervisory authority.
2. Obligation after the termination of personal data processing services
	1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
	2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

IN WITNESS WHEREOF, each of the undersigned entities has caused this Standard Contractual Clauses (Processors) to be signed and delivered by its duly authorized representative.

Dated: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

On behalf of the data exporter:

[This should be completed with the details of the applicable ON Semiconductor entity that is party to the DPA.]

Name of the data exporting organization:

Name:

Address:

Tel: e-mail: Privacy@onsemi.com

Other information necessary in order for the contract to be binding (if any):

Signature

**On behalf of the data importer**:

Name of the data importing organization:

Name:

Address:

Tel. e-mail:

Other information necessary in order for the contract to be binding (if any):

Signature

1. **Description of Transfer**

As set out in Annex 1 above.

**Security Standards**

**Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):**

As set out in Annex 2 above.

1. Internal ON Semiconductor Note to Draft: Applicable entity should be the entity contracting with the vendor. [↑](#footnote-ref-2)
2. For purposes of this DPA, “GDPR” means Regulation (EU) 2016/679 together with any implementing legislation, rules or regulations issued by applicable supervisory authorities. [↑](#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://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill\_id=201720180SB1121 [↑](#footnote-ref-6)
6. Internal ON Semiconductor Note to Draft: Please note that Annex 3 also requires signatures of parties. [↑](#footnote-ref-7)
7. Internal ON Semiconductor Note to Draft: See note above regarding contracting entity. [↑](#footnote-ref-8)
8. Internal ON Semiconductor Note to Draft: Procurement team to coordinate with respect to the applicable vendor arrangement. For reference, special categories of data would include personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data 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. () Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone. [↑](#footnote-ref-10)
10. () Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognized sanctions, tax-reporting requirements or anti-money-laundering reporting requirements. [↑](#footnote-ref-11)
11. () This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision. [↑](#footnote-ref-12)