Realtek Semiconductor Corp.

Personal Data Security Maintenance Policy

Section 1

Realtek Semiconductor Corp. (hereinafter referred to as the “Company”) has established this Policy (hereinafter referred to as the “Policy”) to comply with the Personal Data Protection Act and related laws and regulations governing the collection, processing, and use of personal data.

Section 2

The terms used in this Policy are defined as follows:

1. **Personal Data:** The name, date of birth, national identification number, and any other data that may be used to identify a natural person directly or indirectly.
2. **Personal Data File:** A collection of personal data established in accordance with a system and retrievable or organized by automated machines or other non-automated means.
3. **Collection:** The acquisition of personal data by any means.
4. **Processing:** The recording, input, storage, editing, correction, duplication, retrieval, deletion, output, linkage, or internal transmission of data for the purpose of establishing or using a Personal Data File.
5. **Use:** The use of collected personal data for purposes other than processing.
6. **Government Agency:** A central or local government agency, an administrative corporation, or a quasi-public agency or corporation that exercises public authority in accordance with law or handles affairs under the direction of any of the foregoing agencies or bodies.
7. **Data Subject:** The individual to whom the Personal Data relates.

Section 3

A Data Subject may exercise the following rights with respect to their Personal Data in accordance with this Policy:

1. To make an inquiry or request access.
2. To request a copy.
3. To request supplementation or correction.

Section 4

In using Personal Data, the Company shall respect the rights and interests of the Data Subject, act in good faith, refrain from exceeding the necessary scope of the specific purpose, and ensure that such use has a legitimate and reasonable connection with the purpose for which the Personal Data was collected.

Section 5

The Company shall not collect, process, or use personal data concerning medical records, genetic information, sex life, health examinations, or criminal records in violation of applicable laws and regulations.

1. Where expressly provided by law.
2. Where required by a Government Agency.

3. Where necessary to fulfill legal or regulatory obligations, conduct the Company's operations or management, or provide employee benefits, provided that appropriate security measures are in place.
4. Where the Data Subject has consented, or the Personal Data has been made public or is available through public inquiry.

Section 6

Upon a request from a Data Subject, the Company shall respond to an inquiry, provide access to, or provide a copy of the Personal Data collected about that Data Subject. However, this requirement does not apply under any of the following circumstances:

1. Where doing so would prejudice the Company's confidential information, economic interests, or other material interests.
2. Where doing so would cause the Company to violate its legal or regulatory obligations.
3. Where doing so would prejudice the material interests of a third party.

Section 7

The Company shall maintain the accuracy of Personal Data and shall correct or supplement such data proactively or upon the Data Subject's request.

Section 8

With respect to their Personal Data, a Data Subject may request that the Company respond to an inquiry, provide access to, or provide a copy of such data.

Section 9

For an inquiry or request for access to Personal Data, or a request for a copy, the responsible handling unit may charge the necessary costs.

Section 10

The Company, as the holder of a Personal Data File, shall adopt appropriate security measures to prevent Personal Data from being stolen, altered, damaged, destroyed, lost, or disclosed.

Section 11

To prevent Personal Data from being stolen, altered, damaged, destroyed, lost, or disclosed, the Company shall adopt appropriate technical and organizational security measures.

Section 12

If a Personal Data security incident occurs at the Company, it shall implement emergency response measures and make notifications in accordance with applicable laws and regulations.

Section 13

The Company shall designate the Chief Information Security Officer to convene the Personal Data and Privacy Protection Working Group (as shown in the attached organizational chart). The Working Group shall be responsible for organizing, directing, planning, promoting, and coordinating personal data protection and management matters, as well as the implementation of appropriate security measures. Its responsibilities are as follows:

1. Proposing the Company's personal data protection policy.
2. Promoting the Company's personal data management system.
3. Assessing and managing the Company's personal data risks.
4. Proposing plans to enhance personal data protection awareness and provide education and training for the Company's employees.
5. Assessing the infrastructure supporting the Company's personal data management system.
6. Reviewing, deliberating on, and assessing the legality and appropriateness of the Company's data management system.
7. Other planning matters relating to personal data protection and management.

Section 14

This Policy shall take effect upon approval by the Audit Committee and the Board of Directors. The same shall apply to any amendments to this Policy.

Attachment: Organizational Chart of the Personal Data and Privacy Protection Working Group.

