MAXIM INTEGRATED PRODUCTS, INC.
WORLDWIDE CANDIDATE PRIVACY NOTICE

Contact details: This Worldwide Candidate Privacy Notice ("Notice") addresses the data processing activities by Maxim Integrated Products, Inc. and its affiliates (collectively "we", "us" or "Maxim"), including but not limited to its parent company, Analog Devices, Inc., in relation to Maxim's recruitment process. The local Maxim entity responsible for the job opportunity you are applying for is the joint data controller with Analog Devices, Inc. Maxim processes Personal Data fairly, lawfully, and in accordance with applicable laws, including, the EU General Data Protection Regulation ("GDPR"), the e-Privacy Directive (2002/58/EC), and the California Consumer Privacy Act of 2018 ("CCPA").

- The relevant local Maxim entity is primarily responsible for handling your application and the associated data collection. Analog Devices, Inc. is responsible for the centralized database of applicant's data.

- If you have any questions or complaints in relation to the use of your personal data or this Notice or if you would like to exercise any of your rights (discussed further below), you can contact the HR contact of the local Maxim entity responsible for the job opportunity you are applying for or Maxim's data privacy team at dataprivacy@maximintegrated.com. Contact information for Maxim's current Data Privacy Officers can be found at https://www.maximintegrated.com/en/aboutus/legal/privacy-policy.html.

Personal data collected: We collect the information below about you during the recruitment process. If you fail to provide certain information when requested, we will not be able to progress your application.

- Information provided in your curriculum vitae, application form, covering letter and during the interview process including: your name, date of birth, age, gender, home address, personal e-mail address, education, degrees obtained, university grades, qualification and work experience details, relevant awards, salary information from previous jobs, immigration or visa status (if necessary), and references. We request that you do not disclose sensitive personal characteristics (e.g., height, weight, disabilities, and other health related information, racial or ethnic origin, political opinions, religious or, philosophical beliefs, genetic data, trade union membership, or sexual orientation) as part of your application or in related communications.

    - In some jurisdictions, we may prompt you to voluntarily disclose Equal Employment Opportunity Information ("EEO Information"), including but not limited to, your gender, veteran status, race, ethnicity, and/or disability status.

- Information collected or created by us during the recruitment process including: interview notes, test scores and correspondence between us.

Why we use personal data: We use your personal data to progress the recruitment process, assess and decide about your suitability for a role, to communicate with you and to carry out reference checks. We will also use your information to comply with legal and regulatory requirements. If you are offered a job or become employed by us, the data will be used for other employment-related purposes in accordance with our Employee Privacy Notice (if applicable). Provided EEO Information is only used for diversity tracking/statistics, to comply with legal and regulatory requirements, and for certain positions, to ensure that candidate pools have a minimum number of qualified and diverse candidates. Provided EEO Information is not otherwise used in the recruitment process. We do not sell candidate personal data and have not done so in the past 12 months.

Sources of Information: The information we have is either (a) provided by you; (b) obtained from third parties through the application and recruitment process; or (c) created by us in the course of the recruitment process.

What is the legal basis for using your personal data: We will use the information collected from you because: (1) it is necessary for us to do so before entering into a contract with you at your request; (2) we need to process your information to comply with a legal or regulatory obligation; or (3) because we or a third party have a legitimate interest to: (a) ensure the effective administration and management of the recruitment process; (b) ensure we hire a suitable individual for a role; (c) deal with disputes and accidents and take legal or other professional advice; and (d) ascertain your fitness to work.

Information that we share: As part of the application process for the purposes set out above, we will share your personal data within Maxim and with our service providers. This may involve transferring your data to countries outside your country, including Canada, China, the European Union, Hong Kong, India, Israel, Japan, Korea, Malaysia, Philippines, Russia, Serbia, Singapore, Switzerland, Taiwan, Thailand, Turkey, and the United States.

- We may also share your data with governmental authorities if we are under a legal obligation to do so.

- (EU Only) Where a country has not been deemed to provide an adequate level of protection for personal data by the European Commission in accordance with article 45 GDPR, we will implement appropriate safeguards in accordance with the GDPR. In particular, we use standard contractual clauses in accordance with article 46 GDPR. Where we share data with our service providers, they may be certified under the EU-US

Privacy Shield. If you would like to obtain more information about such safeguards you can request this from us through the contact details above.

- (Other Locations) The data protection laws of other countries might not provide a level of protection equivalent to the laws in your jurisdiction. Maxim will take appropriate steps to ensure such recipients maintain adequate technical and organizational security measures to safeguard your data.

Retention of your information: We will retain your personal data for the duration of the recruitment process and for a reasonable period after the recruitment process has ended, depending on jurisdiction, or through the time period in which you have consented to retention, whichever is later. You can request us to delete your data at any time by emailing dataprivacy@maximintegrated.com. If you are successful in applying for a position, your personal data will be retained in accordance with our Employee Privacy Notice (if applicable).

Your rights: You may have certain rights pertaining to your personal data, which may include access, rectification, erasure, restriction, objection, and data portability. Below we set out your rights under the GDPR (as well as the CCPA where designated) in more detail. These rights are not absolute and are limited by applicable law. In California, you may authorize an agent to make a request on your behalf under the CCPA.

If you wish to exercise any of these rights, please send an email to dataprivacy@maximintegrated.com. We will endeavour to respond to your request within one month but have the right to extend this period if the request is particularly complex or if you submit a large number of requests. If we extend the response period, we will let you know within one month from your request.

- **Access (CCPA)**: you are entitled to ask us if we are processing your information and, if we are, you can request access to your personal data. You may also request information about how we collect, use, and disclose Personal Data.

- **Correction**: you are entitled to request that any incomplete or inaccurate personal data we hold about you be corrected.

- **Erasure (CCPA)**: you are entitled to ask us to delete or remove personal data in certain circumstances (e.g., if you withdrew your consent to process your personal data for specified purposes). There are certain exceptions where we may refuse a request for erasure, for example, where the personal data is required for compliance with law or in connection with claims.

- **Restriction**: you are entitled to ask us to suspend the processing of certain of your personal data about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Portability (CCPA)**: you may request the transfer of certain of your Personal Data to another party. To help with that you have a right to ask that we provide your information in an easily readable format to you or another company.

- **Objection**: where we are processing your personal data based on a legitimate interest (or those of a third party) you may object to processing on this ground. However, we may be entitled to continue processing your information based on our legitimate interests.

Identity Verification for Rights Requests: We may request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. Information received from you for verification purposes will only be used to verify your identity. In certain circumstances, we may request a copy of your government identification to assist us in verifying your identity. We may also contact you to ask you for further information in relation to your request to speed up our response.

Right to withdraw consent: In the limited circumstances where you may have provided your consent to the collection and processing of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time without affecting the lawfulness of processing based on consent before its withdrawal. To withdraw your consent, please send an e-mail to dataprivacy@maximintegrated.com.

Right to lodge a complaint: You also have a right to lodge a complaint with a supervisory authority, in particular in the European Union member state where you are habitually resident, where you work or where an alleged infringement of the data protection laws has taken place.

Non-Discrimination: We will not discriminate against you for exercising any of your data privacy rights under the GDPR, CCPA, or other data privacy laws. In response to an exercise of data privacy rights, we will not:

- Deny you goods or services.
- Charge you different prices or rates for goods or services, including through granting discounts or other benefits, or imposing penalties.
- Provide you a different level or quality of goods or services.
- Suggest that you may receive a different price or rate for goods or services or a different level or quality of goods or services.